



Forensic Dossier User's Manual



Logicube, Inc.
Chatsworth, CA 91311
818 700 8488
www.logicube.com

Version: 2.2
MAN-Dossier
Date: 06/25/2012

Limitation of Liability and Warranty Information

Logicube Disclaimer

LOGICUBE IS NOT LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO PROPERTY DAMAGE, LOSS OF TIME OR DATA FROM USE OF A LOGICUBE PRODUCT, OR ANY OTHER DAMAGES RESULTING FROM PRODUCT MALFUNCTION OR FAILURE OF (INCLUDING WITHOUT LIMITATION, THOSE RESULTING FROM: (1) RELIANCE ON THE MATERIALS PRESENTED, (2) COSTS OF REPLACEMENT GOODS, (3) LOSS OF USE, DATA OR PROFITS, (4) DELAYS OR BUSINESS INTERRUPTIONS, (5) AND ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE (OR FROM DELAYS IN SERVICING OR INABILITY TO RENDER SERVICE ON ANY) LOGICUBE PRODUCT.

LOGICUBE MAKES EVERY EFFORT TO ENSURE PROPER OPERATION OF ALL PRODUCTS. HOWEVER, THE CUSTOMER IS RESPONSIBLE TO VERIFY THAT THE OUTPUT OF LOGICUBE PRODUCT MEETS THE CUSTOMER'S QUALITY REQUIREMENT. THE CUSTOMER FURTHER ACKNOWLEDGES THAT IMPROPER OPERATION OF LOGICUBE PRODUCT AND/OR SOFTWARE, OR HARDWARE PROBLEMS, CAN CAUSE LOSS OF DATA, DEFECTIVE FORMATTING, OR DATA LOADING. LOGICUBE WILL MAKE EFFORTS TO SOLVE OR REPAIR ANY PROBLEMS IDENTIFIED BY CUSTOMER, EITHER UNDER WARRANTY OR ON A TIME AND MATERIALS BASIS.

Warranty

LOGICUBE PROVIDES A BASIC ONE-YEAR PARTS AND LABOR WARRANTY FOR ALL OF ITS PRODUCTS (EXCLUDING CABLES, ADAPTERS AND OTHER "CONSUMABLE" ITEMS). A TWO-YEAR EXTENDED WARRANTY IS ALSO AVAILABLE FOR AN ADDED COST. TELEPHONE AND EMAIL SUPPORT IS AVAILABLE FOR THE LIFE OF THE PRODUCT AS DEFINED BY LOGICUBE.

RoHS Certificate of Compliance

LOGICUBE PRODUCTS COMPLY WITH THE EUROPEAN UNION RESTRICTION OF THE USE OF CERTAIN HAZARDOUS SUBSTANCES IN ELECTRONIC EQUIPMENT, ROHS DIRECTIVE (2002/95/EC).

THE ROHS DIRECTIVE PROHIBITS THE SALE OF CERTAIN ELECTRONIC EQUIPMENT CONTAINING SOME HAZARDOUS SUBSTANCES SUCH AS MERCURY, LEAD, CADMIUM, HEXAVALENT CHROMIUM AND CERTAIN FLAME-RETARDANTS IN THE EUROPEAN UNION. THIS DIRECTIVE APPLIES TO ELECTRONIC PRODUCTS PLACED ON THE EU MARKET AFTER JULY 1, 2006.

Logicube Declaration of Conformity



Logicube declares that this product meets all appropriate EUROPEAN UNION health, safety, and environmental requirements, which ensure consumer and place safety. It is in compliance with all requirements and provisions of Directive 36/EEC, and all other relevant directives.
PLEASE CONTACT LOGICUBE, INC. FOR A COPY OF THIS DECLARATION.

Logicube Technical Support Contact Information

1. By website: www.logicube.com
2. By email: techsupport@logicube.com
3. By telephone: 1 - (818) 700 8488 ext. 3 between the hours of 8am –6pm PST, Monday through Friday, excluding U.S. legal holidays.

Table of Contents

FORENSIC DOSSIER USER'S MANUAL	I
LIMITATION OF LIABILITY AND WARRANTY INFORMATION	II
LOGICUBE DISCLAIMER	II
WARRANTY	II
ROHS CERTIFICATE OF COMPLIANCE	III
LOGICUBE DECLARATION OF CONFORMITY	III
LOGICUBE TECHNICAL SUPPORT CONTACT INFORMATION	III
TABLE OF CONTENTS	IV
1. INTRODUCTION TO THE FORENSIC DOSSIER	9
INTRODUCTION	9
SPECIFICATIONS	9
FEATURES	10
USING THIS GUIDE	11
SYSTEM DESCRIPTION	12
2. GETTING STARTED	16
DRIVE NAMES AND LOCATIONS	16
SETTING UP THE LOGICUBE DOSSIER	17
<i>Opening the Logicube Dossier</i>	17
<i>Connecting a PATA Drive</i>	18
<i>Connecting a Serial ATA (SATA) Drive</i>	20
<i>Connecting other types of drives</i>	21
THE USER INTERFACE	22
TOUCH SCREEN	22
<i>Calibrating the Touch Screen</i>	22
DATE & TIME	23
E01 RESUME (INCOMPLETE SESSIONS)	24
BUTTONS	24
ALPHANUMERIC KEYPAD	25
INDICATOR LIGHTS	25
3. DRIVE CAPTURE MODES AND SETTINGS	26
MAIN SCREEN	26
<i>Misc</i>	26
<i>Drives</i>	26
<i>Settings</i>	27
<i>About</i>	27
MODES OF OPERATION	27
CAPTURING A DRIVE	28
TO PERFORM A MIRROR CAPTURE	29

TO PERFORM A DD IMAGE CAPTURE	31
SPECIAL SETTINGS FOR DD IMAGE MODE	33
<i>Verify Disk or File</i>	33
<i>File Size</i>	33
LOADING DD IMAGE FILES INTO A FORENSIC INVESTIGATIVE TOOL.....	33
E01 IMAGE	34
TO PERFORM AN E01 IMAGE CAPTURE	34
SPECIAL SETTINGS FOR E01 IMAGE MODE	37
PRINTING A REPORT	38
PRINTING WITH THE BROTHER (THERMAL) PRINTER	38
OPTIONAL PREFERENCE SETTINGS	39
MODE.....	39
VERIFY	40
SPEED	40
ON ERROR	42
WORD LIST	43
MODIFY LIST	43
CAPTURING DATA FROM HPA AND DCO CONFIGURATIONS.....	43
4. OTHER MODES	45
INTRODUCTION.....	45
SETTINGS MENU OPTIONS.....	45
DRIVE DEFECT SCAN	45
<i>Procedure</i>	45
WIPE DESTINATION	46
<i>Procedure</i>	46
HASH SCAN	48
<i>Procedure</i>	48
MISC MENU SETTINGS	49
BACKLIGHT	49
AUTHENTICATE TRAIL	49
<i>Procedure</i>	49
MANAGE SETTING	50
<i>Contrast</i>	50
<i>Save Settings</i>	50
<i>Factory Settings</i>	50
MANAGE DESTINATION.....	50
PRINT OPTIONS	52
<i>Eject Page</i>	52
<i>Print Report</i>	52
<i>Auto Print (After Capture)</i>	52
DEBUG	53
BEEPER.....	53
AUDIO NOTICE FOR ERROR.....	53
SECURITY	53
<i>High Security</i>	54
<i>Maximum Security</i>	54
<i>Type</i>	54
<i>Get</i>	56
<i>Disabled</i>	56
SCSI/SAS ADAPTER	57
<i>Performing SAS and SCSI Adapter Updates</i>	57
RETRY	60

INSTALL OPTIONS	60
FILE SYSTEM	60
LANGUAGES.....	61
TIME ZONE	61
E01 RESUME	61
DAYLIGHT SAVING.....	62
5. CAPTURING RAID CONFIGURATIONS	63
INTRODUCTION.....	63
SOURCE DRIVE CLONING NOTES	64
<i>Drive Capture and DD Capture</i>	<i>64</i>
<i>Verify.....</i>	<i>64</i>
<i>Calculate HASH and Keyword Search</i>	<i>64</i>
OTHER NOTES.....	64
6. USB AND FIREWIRE PORTS	65
INTRODUCTION.....	65
MINIMUM REQUIREMENTS.....	65
USB CONNECTION TO WINDOWS (FOR DRIVE MANAGEMENT).....	66
FIREWIRE CONNECTION TO WINDOWS (FOR DRIVE MANAGEMENT)	67
REMOVING USB DEVICES.....	68
CLONING THROUGH THE USB/FIREWIRE PORTS	68
<i>How to set up and use the USB/FireWire cloning software:</i>	<i>69</i>
<i>Selectable Capture Modes & Options</i>	<i>70</i>
<i>Cloning a Mac using FireWire and the Cloning Software:</i>	<i>73</i>
<i>Additional Notes</i>	<i>73</i>
7. KEYWORD SEARCHING	75
INTRODUCTION.....	75
SEARCHING FOR KEYWORDS	75
SEARCHING DURING CAPTURE	75
SEARCHING WITH KEYWORD SEARCH MODE.....	76
<i>Procedure</i>	<i>76</i>
KEYWORD LISTS.....	77
MODIFY LIST SETTINGS	78
MODIFY LISTS.....	78
8. OPTIONAL PERIPHERALS	82
INTRODUCTION.....	82
MASSIVE PORTABLE FORENSIC STORAGE (MPFS™)	82
FEATURES.....	83
SYSTEM DESCRIPTION	83
CONNECTING THE FORENSIC DOSSIER TO THE MPFS	84
NETCONNECT™	86
FEATURES.....	86
CONNECTING NETCONNECT TO THE FORENSIC DOSSIER TRAY	86
LOGICUBE CLONE CARD PRO™	88
BEFORE CAPTURING	89
USING THE LOGICUBE CLONECARD PRO TO CAPTURE A DRIVE.....	89
IMPROVING SPEED OF TRANSFER	90
LOGICUBE PORTABLE BATTERY PACK.....	91
PRECAUTIONS	91
WHAT'S INCLUDED	91

CHARGING THE BATTERY – DOS & DON'TS	91
CONNECTING BATTERY TO CHARGER	91
CONNECTING BATTERY & DEVICE	92
CONNECTING MULTIPLE BATTERIES	93
ADDITIONAL CONSIDERATIONS	93
WASTE DISPOSAL METHOD	93
LOGICUBE SCSI ADAPTER	94
WHAT'S INCLUDED	94
WHAT'S NEEDED	94
INSTALLATION SETUP	95
HOW TO USE THE SCSI ADAPTER	95
DUPLICATING USING FORENSIC DOSSIER	95
OPTIONAL USB CLONING WITH THE SCSI ADAPTER	96
LOGICUBE SAS ADAPTER	97
WHAT'S INCLUDED	98
WHAT'S NEEDED	98
INSTALLATION SETUP	98
HOW TO USE THE SAS ADAPTER	99
DUPLICATING USING FORENSIC DOSSIER	99
OPTIONAL USB CLONING WITH THE SAS ADAPTER	99
9. INTERNAL FLASH MEMORY	101
INTRODUCTION	101
CONNECTING THE CF DRIVE TO WINDOWS VIA USB OR FIREWIRE	101
CONNECTING THROUGH USB OR FIREWIRE MODE	101
REMOVING USB DEVICES	102
INSTALLATION AND REMOVAL OF INTERNAL CF DRIVE	102
INTERNAL FLASH MEMORY REMOVAL AND INSTALLATION	102
10. SOFTWARE AND FIRMWARE LOADING INSTRUCTIONS	104
INTRODUCTION	104
LOADING NEW SOFTWARE AND FIRMWARE	104
MPFS (MASSIVE PORTABLE FORENSIC STORAGE) NOTES:	105
11. REFERENCE	107
FURTHER NOTES ON MODES AVAILABLE FOR THE DOSSIER	107
CAPTURE – NATIVE OR DD IMAGE	107
DRIVE DEFECT SCAN	107
<i>Options</i>	107
WIPE DESTINATION	107
<i>Options</i>	107
<i>Erase process with Security Erase</i>	108
<i>Erase process using non Security Erase drives</i>	108
ADDITIONAL COMMANDS	108
VERIFY	108
<i>HASH</i>	108
<i>HASH + V</i>	108
<i>None</i>	108
ON ERROR	109
PRINTER	110
ANATOMY OF A DRIVE CAPTURE	110
POWER-UP AND INITIALIZATION	110
LOG FILE NAME ENTRY	111

CALIBRATE TRANSFER SPEED	111
CHECK CAPTURE INTEGRITY.....	112
VERIFY DESTINATION DRIVE IS ERASED	113
VERIFY ERASURE.....	113
WIPE DESTINATION	113
<i>Erase Process</i>	113
<i>Write a unique signature to the destination drive.</i>	113
CAPTURE SOURCE DRIVE DATA TO DESTINATION DRIVE	114
CHECK FOR ERASURE OF UNUSED PORTION OF DESTINATION DRIVE	114
PRINT FINAL CAPTURE REPORT	114
FINAL CAPTURE REPORT (HARDCOPY PRINTOUT)	114
<i>Information Format</i>	114
EXAMPLE OF HARDCOPY PRINTOUT	118
12. FREQUENTLY ASKED DOSSIER QUESTIONS AND ANSWERS.....	119
13. INDEX	121
TECHNICAL SUPPORT INFORMATION.....	123

1. Introduction to the Forensic Dossier

Introduction



Thank you for purchasing the Logicube Forensic Dossier. With proper use, this unit will provide you with accurate HDD capturing for years to come.

The Logicube Forensic Dossier is a drive-to-drive duplication device. Typically, a suspect hard drive and a destination drive will be connected to the unit. Within minutes of starting the process, the contents of the suspect drive are accurately copied over to the target drive for further examination. Handling of the suspect drive is held to a minimum with zero alteration of its contents.

Designed with the Forensics investigator in mind, the system ensures that proper evidence capture procedures are maintained, while speeding up the process significantly.

Specifications

The Forensic Dossier represents the sixth generation of computer forensic solutions from Logicube and is designed to meet the complex challenges of digital forensic investigations. This high speed, handheld

solution allows users to quickly capture data from SATA/PATA hard drives and a variety of flash media devices. Optional support for capture from SCSI and SAS hard drives is available. The Dossier can capture data from one or two suspect drives to either one or two evidence drives simultaneously. This feature allows investigators to quickly acquire potential evidence from multiple suspect hard drives and create multiple copies of the suspect drive to speed the analysis process.

Power Requirements	90 to 240VAC 50 to 60Hz
Power Consumption	<150 watts
Operating Temperature	10°-35°C (50°-95°F)
Relative Humidity	10%-80%
Net Weight	2lb 13oz
Dimensions	10.6" W x 8.5" H x 3" D
Agency Approvals	RoHs compliant FCC Part 15 Class A, CE

Features

- Built-in support for capture from SATA/PATA hard drives, flash media and RAID drive pair
- Optional support for capture from SCSI and SAS hard drives
- Optional support for capture to E01 File Format
- Ability to compute SHA-256 and MD5 Hash concurrently in real time (at full Capturing speed).
- Able to Capture 1 or 2 suspect drives to 1 or 2 Destination drives. This allows batch capturing, capturing from RAID drives or making two destination drive copies at once.
- Spanning mode allows you to capture from one large suspect drive to two smaller evidence drives
- Able to capture data directly from six different flash media types to 1 or 2 destination drives.
- Keyword search capabilities – Search for hundreds of words concurrently on a hard drive; either during the capture process, or on a single drive. Specify: upper-case, case-sensitive, Unicode, start of sector, and regular text.

- DD image capture mode – Capture a suspect's hard drive to multiple DD image files. User specified file size of: 650MB, 2GB, and 4GB, for later archiving on to other media like CDs, DVDs, or Flash Memory.
- Destination drives fit seamlessly inside Dossier with a unique "slide-in" design.
- Wipe feature; wipe two drives simultaneously
- Write-protected data transfer to prevent overwriting
- Captures from DCO and HPA areas of the hard drive
- Audit trail reporting. Generate and write to a System Compact Flash card for review and printing
- Internal System Compact Flash memory – Stores keyword lists, software updates, reports etc. Accessible via USB or FireWire (1394).
- Capture from an unopened desktop/laptop PC or MAC (except MacBook Air) with the Forensic USB/FireWire Cloning Software (included on a CD-ROM with the Dossier)
- High-speed acquisition of USB enclosures, USB external drives, or USB flash drives available with an optional software key code and either the SCSI or SAS adapter
- Fully integrated QWERTY keypad – For easy entry of file names, user passwords, keyword lists, etc.

Using this guide

This user guide is made up of 11 sections:

- Introduction
- Getting Started (Fast Start)
- Drive Capture Modes and Settings
- Other Modes
- Capturing RAID Configurations
- USB and FireWire Connection
- Keyword Searching
- Optional Peripherals
- Internal Flash Memory
- Software and Firmware Loading Instructions
- Reference / FAQ's / Index

Please read **Chapter 1: Introduction** and **Chapter 2: Getting Started** before attempting a drive capture. It is recommended that you practice with a test or scratch drive to fully appreciate the unit's features.

System description

The Forensic Dossier Standalone system is packed in a rugged carrying case. Inside, you will find the following components:

- The Logicube Forensic Dossier with power adapter.
- 4 drive power cables, 2 short and 2 long (used to connect PATA suspect and destination drives to the unit).
- 4 HDD (Hard Disk Drive) data cables, 2 short and 2 long (used to connect PATA drives to the unit).
- Two Serial ATA data/power cables for attaching Serial ATA (SATA) suspect drives to the unit.
- A "Mini-B" USB cable that allows the unit to be connected to the USB port of a PC.
- 1 FireWire (IEEE 1394) cable that allows the unit to connect to the FireWire port of a PC.
- A flashlight and screwdriver.
- A CD-ROM that contains the Forensic USB/FireWire Cloning Software
- A CD-ROM that includes:
 - A utility program to load the Forensic Dossier with new software.
 - A backup copy of the current Forensic Dossier software.
 - Extra copies of all files found on the internal Flash memory.
 - This manual in electronic form.
- A carrying case.

NOTE: It is recommended that you always use the carrying case to store and carry the unit.

The Forensic Dossier Kit is packed in a rugged, carrying case. Inside, you will find the following components:

- The Forensic Dossier with power supply.
- E01 option enabled (included with kits purchased after October 2009).

- 4 drive power cables, 2 short and 2 long (used to connect PATA suspect and destination drives to the unit).
- 4 HDD (Hard Disk Drive) data cables, 2 short and 2 long (used to connect PATA drives to the unit).
- Two Serial ATA data/power cables for attaching Serial ATA (SATA) suspect drives to the unit.
- One set of extra-long PATA cables (18") to allow drive capture without removing the drive from a PC chassis.
- One set of extra-long SATA cables (18") to allow drive capture without removing the drive from a PC chassis. (included with kits purchased and shipped effective October 14, 2009)
- One eSATA cable (included in kits with purchased and shipped effective October 14, 2009)
- One MicroSATA cable (included in kits purchased and shipped effective October 2009)
- One 2.5" drive adapter to allow the connection of 2.5" PATA drives (F-ADP-STND).
- One 1.8" PATA drive adapter for 1.8" PATA drives (F-ADP-1.8).
- One ZIF adapter for 1.8" drives with a ZIF connector (F-ADP-ZIF).
- One Logicube CloneCard Pro™ – A Type-II 16-bit PCMCIA card with a bootable CD-ROM containing a client application. This is used for capturing data from older notebook PCs.
- A "Mini-B" USB cable that allows the unit to be connected to the USB port of a PC.
- 1 FireWire (IEEE 1394) cable that allows the unit to connect to the FireWire port of a PC.
- A flashlight and screwdriver.
- A CD-ROM that contains the Forensic USB/FireWire Cloning Software
- A CD-ROM that includes:
 - A utility program to load the Forensic Dossier with new software.
 - A backup copy of the current Forensic Dossier software.
 - Extra copies of all files found on the internal Flash memory.

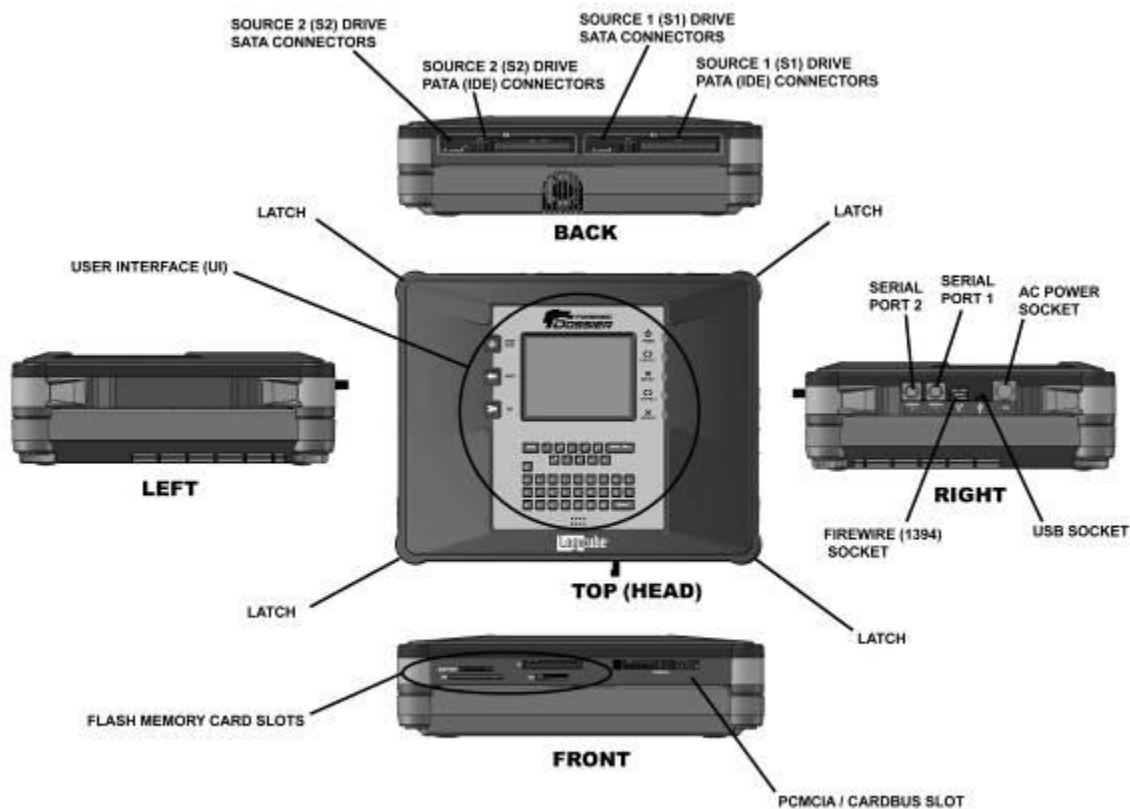
– This manual

- A rugged carrying case.

NOTE: It is recommended that you always use the carrying case to store and carry the unit.

Caution: Incorrectly connecting the suspect drive to the system can result in data on the suspect drive to be lost forever. **Never place a suspect drive inside the Forensic Dossier as data may be overwritten.**

Caution: Never place a suspect drive into any other Logicube products (e.g. Sonix™) that are used for Operating System cloning.



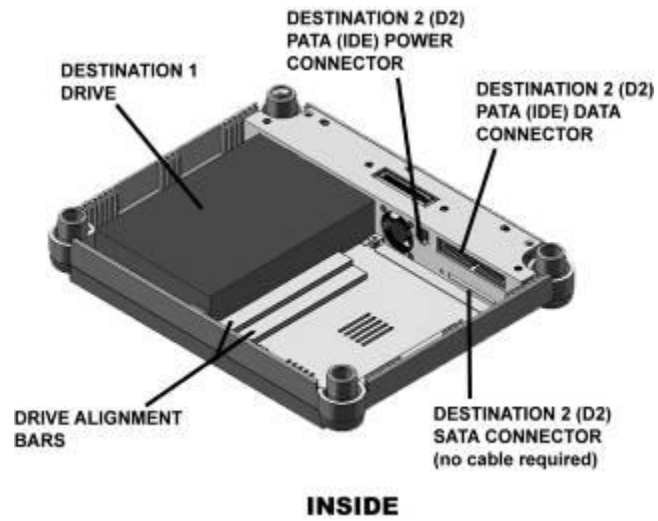


Figure 1, Forensic Dossier

2. Getting Started

Drive Names and Locations

The following naming conventions will be used throughout this manual:

Hard disk drives attached inside the Dossier are always referred to as **Destination** (or **Evidence**) drives and the outside drives are always referred to as the **Source** (or **Suspect**) drives. Flash memory cards are also referred to as **Flash** drives.

PATA (Parallel-ATA) will be used instead of the older term, IDE or E-IDE.

Also, positions for Source drives are referred to as **S1** (left) and **S2** (right). Destination drive positions are **D1** (left) and **D2** (right). Please see Fig. 2 below:

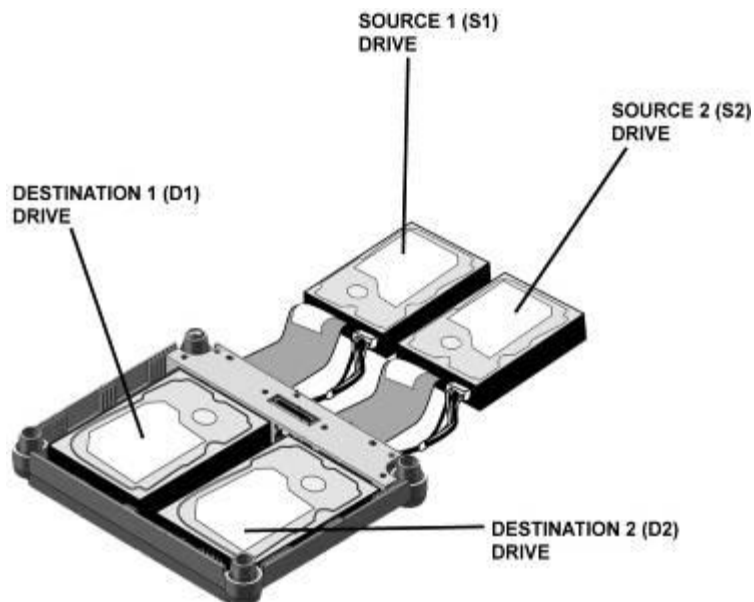


Figure 2, Drive Locations

Setting Up the Logicube Dossier

The Logicube Dossier is able to detect whether Parallel ATA (commonly known as IDE) or Serial ATA (SATA) drives are attached to any of the Source or Destination positions. The unit is capable of cloning to SATA drives from PATA drives and vice versa (as well as PATA to PATA and SATA to SATA). Flash Media Cards are also detected as an available source upon insertion.

NOTE: Never attach both a PATA and SATA drive to a single Source or Destination position. The unit can only handle one drive on each position. It is perfectly fine to attach a PATA drive to one position (i.e. D1) and a SATA drive to the other position (i.e. D2).

The unit can also detect if a Flash memory card is present in one of the four memory slots. The unit can capture data from one flash memory card to one or two destination drives.

NOTE: The Mode of the Dossier will determine which source is to be captured therefore it is safe to attach more than one Flash memory card to the Dossier at a time.

Before applying power perform the steps listed below:

Opening the Logicube Dossier

Destination drives are attached to the inside of the Logicube Dossier. Follow these steps to open the unit:

1. Turn the tabs on each corner of the unit as shown in Fig. 3 below:



Figure 3, Opening corner latches.

2. Lift the top (or “head”) off the bottom of the unit as show in Fig. 4 below:

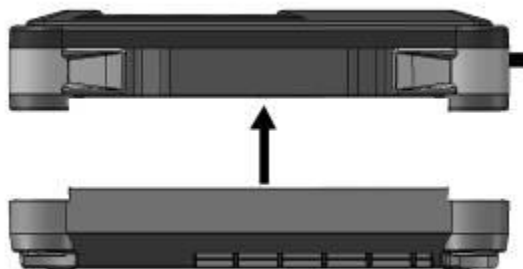


Figure 4, Lifting head off unit.

Connecting a PATA Drive

1. Open the Logicube Dossier by turning the tabs on all four latches at the corners of the unit and lifting the top off. You will notice three connections at each Destination drive position: One for a flat cable (the drive data cable) and another for a small drive power cable. Underneath is the SATA connection.

Note: When connecting the data and power cables, ensure that the flat data ribbon loops on the upper side of the destination drive by carefully sliding the drive under both cables. See Figure 5, “Connecting Destination drives to the Logicube Dossier through 5” Data/Power cables”.

2. Connect one or two Destination hard drives and close the Logicube Dossier.
3. Plug in the set of 9” cables, to the connections found on the back of the Logicube Dossier.

Note: See Figure 6, “Connecting Source drives to the Logicube Dossier through 9” data/power cables”.

4. Connect one or two Suspect drives to these cables.

Note: Internal drives are always referred to as the **Destination** (or **Evidence**) drive and the outside drives are always referred to as the **Source** (or **Suspect**) drives.

5. Connect the external power supply to the Logicube Dossier and power-up the unit. In 4 – 5 seconds, the main “Splash” screen appears.

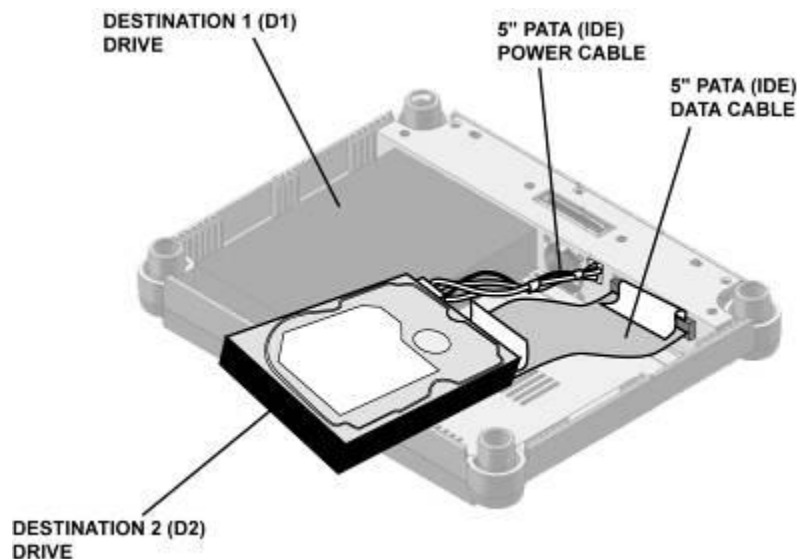


Figure 5, Connecting Destination drives to the Logicube Dossier through 5" Data/Power cables.

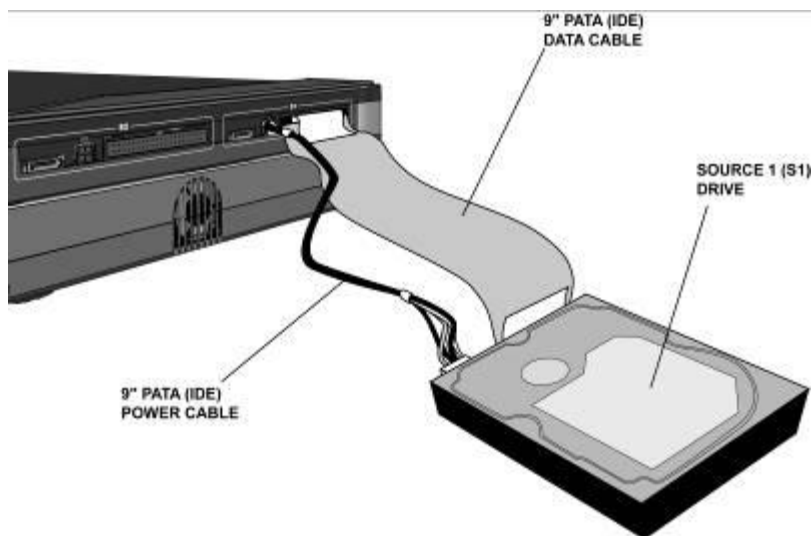


Figure 6, Connecting Source drives to the Logicube Dossier through 9" data/power cables.

Note: In order for a capture to work, most PATA drives must be configured as a master drive. If you are going to capture a drive that is used as a slave, move the jumper to the master position. Before moving a jumper note its position so you can return the suspect drive to its original state when the capture operation has been completed.

Note: There are some drives that do not follow the requirement stated above. Those drives are:

- **Western Digital** – Most Western Digital drives require that the jumpers be removed for a capture to work. The exception to this requirement is for the Western Digital “Xpert” series hard drives (an older manufactured version) where the jumper is set to the master position.
- **Quantum** - The jumper must be placed in the “DS” position. The “DS” position is adjacent to the 40-pin connector. See figure 7.

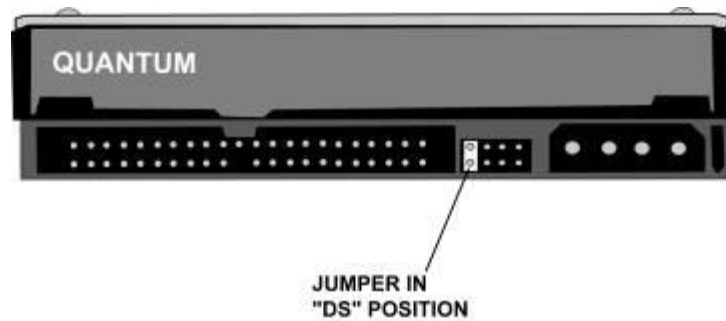


Figure 7, DS Position

Connecting a Serial ATA (SATA) Drive

1. Open the Logicube Dossier by turning the tabs on all four latches at the corners of the unit and lifting the top off. You will notice three connections at each Destination drive position: One for a flat cable (the drive data cable) and another for a small drive power cable. Underneath is the SATA connection.

Note: The UDMA drive data and power cables must be removed from the Dossier when a SATA drive is connected.

Note: See Figure 8, “Connecting SATA Destination drives to the Logicube Dossier”.

2. Connect one or two Destination hard drives and close the Logicube Dossier.
3. Plug in the long SATA cable to the connections found on the back of the Logicube Dossier.

Note: See Figure 9, “Connecting SATA Source drives to the Logicube Dossier through a 9” SATA cable”.

4. Connect the Source drive to this cable.

Note: The internal drive is always referred to as the **Destination** (or **Evidence**) drive and the outside drive is always referred to as the **Source** (or **Suspect**) drive.

5. Connect the power supply to the Logicube Dossier and power-up the unit. In a few seconds, the main display appears.

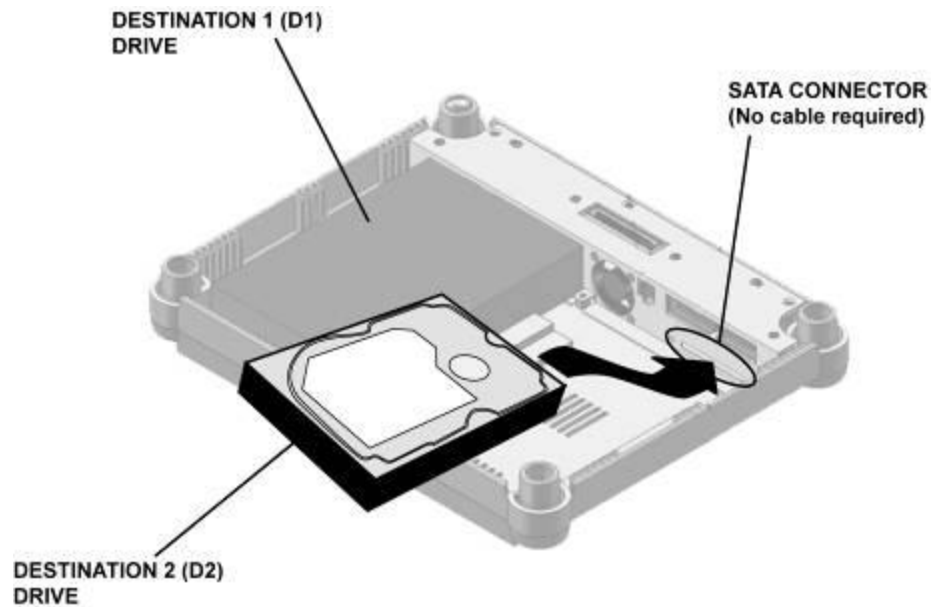


Figure 8, “Connecting SATA Destination drives to the Logicube Dossier”.

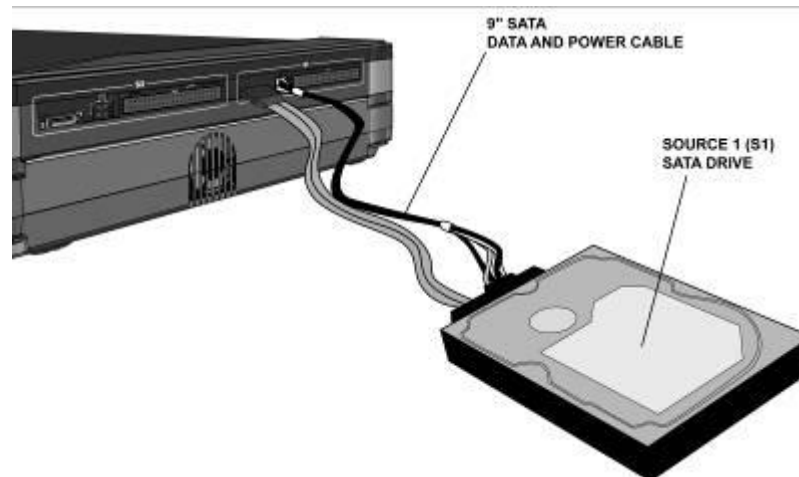


Figure 9, Connecting SATA Source drives to the Logicube Dossier through a 9" SATA cable.

Connecting other types of drives

Logicube sells specialized adapters that allow other types of drives to be connected to the Logicube

Dossier. Such drives include 2.5" PATA (IDE) drives, 1.8" PATA (IDE) or SATA drives and USB drives.

Other specialized adapters are also available. If you are unsure about the type of drive that you have, please contact Logicube Technical Support for assistance.

Note: SCSI and SAS drives cannot be connected directly to the Logicube Dossier.

The user interface

The user interface (UI) has been re-designed with the professional in mind. It is fast, responsive, and to the point; which means it requires very few keystrokes to achieve a desired action.

NOTE: Please refer to Fig. 10 as you read the information below.

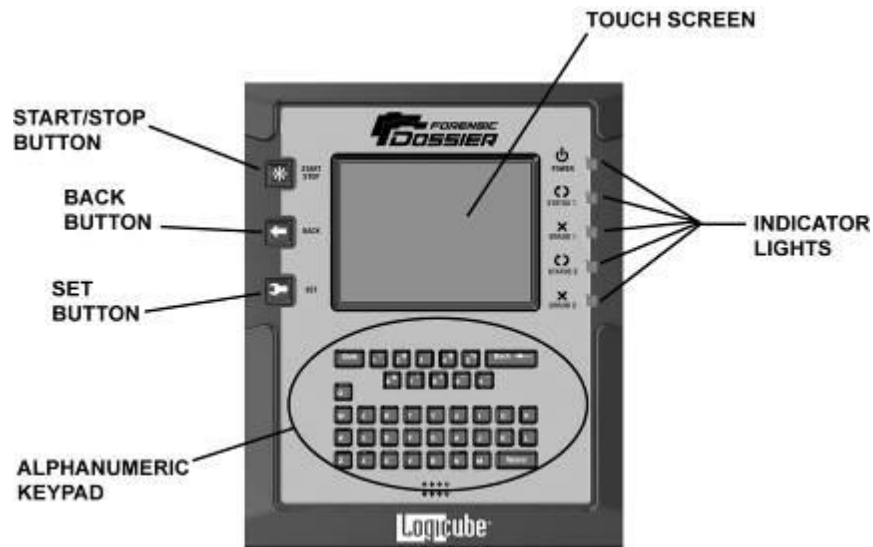


Figure 10, Buttons and Interface

Touch Screen

The Dossier features an LCD Touch Screen that allows the user to quickly input commands. This screen replaces many of the buttons that were present on older Logicube forensic products. The screen is bright and easy to read. It also has an audible beep every time the touch screen is pressed. This lets the user know that the touch screen is active and can be turned off, if desired.

Calibrating the Touch Screen

There may be times when the user wants to recalibrate the Touch Screen. The procedure for

this is very simple as outlined in the procedure below:

1. Unplug the power adapter from the Dossier to turn it off.
2. Press and hold the **SET** button, then plug the Dossier power adapter back in.
3. Hold the **SET** button until the Dossier boots to a screen that reads "Touchpad Calibration. Touch the center of square (1/5)".

NOTE: You can also calibrate the touch screen with a stylus or the dull plastic tip of a writing instrument. Do not use any writing instrument that will leave marks on the unit.

4. Look for a square at the top of the screen. Touch the square when it is located.
5. Repeat the previous step four more times. The unit will count each time the square is pressed correctly. It will count (1/5), (2/5), etc.
6. Once the screen has been calibrated, it will show the Main Menu Screen.

Date & Time

This feature is available with software version 2.1.0RC14 and above.

The real time clock is displayed on the Main Menu screen and will add a time stamp to the log files created by the Dossier in two locations.

The top of the report will contain the date and time the capture process was started. The end time of the capture process will be shown on the bottom of the report and is only available when using DD Image or E01 Image Captures.

The time can be adjusted by setting the correct Time Zone along with the Daylight Savings setting. Please refer to **Time Zone** and **Daylight Savings** in the **Misc. Menu** section of **Chapter 4: Other Modes** for more information on these two settings.

DATE & TIME NOTES:

1. If you Dossier's serial number is 79000 and above and you do not see the real time clock on the Main Menu screen, check your software version by tapping "About" from the Main Menu. The real time clock is available with software version 2.1.0RC14 and newer. If your software version is below 2.1.0RC14, download and install the latest software from Logicube's website.

2. If your Dossier's serial number is below 79000 and you do not see the real time clock on the Main Menu screen, check your software version by tapping "About" from the Main Menu. The real time clock is available with software version 2.1.0RC14 and newer. If your software version is below 2.1.0RC14, download and install the latest software from Logicube's website. If after updating the software and you still do not have the date & time on the Main Menu screen, please contact Logicube Technical Support via telephone at 818-700-8488, option 3 or by email: support@logicube.com.

E01 Resume (Incomplete Sessions)

This feature is available with software version 2.1.0RC14 and above.

When an E01 capture is being performed and the capture process is interrupted (for example, the AC adapter was disconnected or the power switch accidentally turned off), the Forensic Dossier has the ability to resume the unfinished capture. When this occurs, the Forensic Dossier will boot to a special screen that states:

Found Incomplete Session

This screen will contain the case name that was used before the session was interrupted along with the capture mode and status. On this screen, there are three options:

Don't ask – Selecting this option will place a check mark on the box. This will instruct the Dossier to no longer show you the resume screen for this capture. Unless this option is checked, the 'Found Incomplete Session' screen will come up every time the Dossier is turned on.

Res – Resume button. Selecting this will resume the E01 capture that was interrupted.

Skip – This button will skip the resume function allowing you to either start from the beginning or start a different capture.

NOTE: There is a way to go back and resume previously skipped sessions even after 'Don't ask' was checked. For more information on viewing previously skipped sections, see the **E01 Resume** section in **Chapter 4: Other Modes**.

NOTE: When resuming an incomplete session, the same Source and Destination drive(s) must be attached to the Dossier. An error will appear if the serial numbers of the Source or Destination drive(s) do not match.

Buttons

The Dossier features three buttons that are located to the left of the touch screen.

- **START/STOP Button** – Pressing this button twice from the Main Menu to begin a DD Image Capture using the currently saved settings. Pressing and holding down the START/STOP button in the middle of a capture will abort the process. Pressing this button once presents a preview screen where you can decide whether to press it again to begin the selected process, or back out to reconfigure.
- **BACK Button** - This button is used to go back to the previous screen or to cancel out of a given operation.
- **SET Button** – Hold this button while powering up the Dossier for screen calibration or to finalize log file names. The Set button is also used extensively in some menu settings like Keyword Search and Calculate Hash.

Alphanumeric Keypad

The alphanumeric keypad is used for labeling capture sessions, entering passwords and other functions.

Indicator Lights

The indicator lights are located to the right of the touch screen.

The **POWER** indicator light remains on while the Logicube Dossier is receiving power.

The **STATUS** indicators are lit during cloning operations and any operation that accesses the Source or Destination drives. They will flash as data is transferred from one drive to the other.

The **STATUS 1** light is for the S1 and D1 drives. The **STATUS 2** light is for the S2 and D2 drives. Capturing a Flash drive uses the **STATUS 1** light.

The **ERROR** light will turn on if a problem is encountered during cloning or any other operation. If this occurs, check the screen for an error message and instructions on what to do next.

The **ERROR 1** light is for the S1 and D1 drives. The **ERROR 2** light is for the S2 and D2 drives. Capturing a Flash drive uses the **ERROR 1** light.

3. Drive Capture Modes and Settings

Main Screen

The main menu screen appears when the Logicube Dossier is first powered up. It displays the Title Screen and four menu options: **Misc**, **Drives**, **Settings**, and **About**.



Misc

Tap the **Misc** icon to access the following functions:

- Backlight (on or off)
- Authenticate Trail
- Manage Settings
- Manage Destination menu
- Print Options menu
- Debug (on or off)
- Beeper (on or off)
- Audio Notice (on or off)
- Security
- SCSI/SAS Adapter
- Retries (adjustable)
- Install Options

These options are explained in more detail under **Chapter 4: Other Modes**.



Drives

Tap the **Drives** icon. Another screen will come up asking you to select Either S1, S2, D1, D2 or Flash depending on what is connected to the unit. Make your choice by tapping the desired drive's icon. The unit will then access the drive selected and report back the drive's model number, capacity, geometry and other information.

Settings



Tap the **Settings** icon to access the settings screen.

NOTE: All of the features available in the Settings menu are explained starting on the next section.

About



Tap the **About** icon to display the serial number of your unit along with the software and firmware versions that are loaded. In addition, the About screen provides contact information for Logicube Technical Support.

Modes of Operation

The Logicube Dossier supports three different operations to capture data from a suspect drive: **Mirror Capture**, **DD Image Capture**, and **E01 Image Capture**. These modes are found in the Settings Menu along with several other operations. The different modes of operation are briefly described below.

NOTE: Each time the Logicube Dossier is powered off, the cloning mode and preference settings are returned to their factory defaults.

The following Modes of Operation are found in the Mode Setting Menu:



- **Capture** – This process captures all data from the source drive to the destination drive. This mode is also called a “Native Capture” or “Mirror Capture” since data is captured at the sector level to one or two destination drives.



- **DD Image** – This mode of capturing creates a subdirectory per drive captured, with DD style files of size 650 MB, 2 GB, or 4 GB each. These files are directly accessible by popular Forensic analysis software tools, such as, Encase, FTK, and iLook.



- **E01 Image** – The E01 option captures hard disk drives directly into the E01 format. The evidence or destination drive can then be easily uploaded to the analysis software in a ready-to-analyze state. This eliminates the time consuming conversion step that users typically must perform today.



- **Drive Defect Scan** – This operation performs a surface scan of the drive media using the drive controller to verify the media, and detect bad or “weak” sectors. This mode is described in **Chapter 4. Other Modes**.



- **Wipe Destination** – This is used to erase all data on the destination drive prior to a Native Capture. This mode is described in **Chapter 4: Other Modes**.



- **Calculate HASH** – This is used to compute SHA-256 and MD5 values of the source, destination or flash drives. This mode is described in **Chapter 4: Other Modes**.



- **USB / 1394** – This mode is used to connect the Dossier to a PC through the USB or FireWire (1394) port. This mode also needs to be engaged when attempting a capture through the USB or FireWire port. This mode is described in **Chapter 6: USB and FireWire Connection**.



- **Keyword Search** – Used to perform a binary or hexadecimal keyword search on a given drive. This mode is described in **Chapter 7: Keyword Search**.

Capturing a Drive

Connect the drives as previously described. Make sure the destination drive is larger in capacity than the suspect drive (source drive).

NOTE: For Mirror Capture, the Source and Destination drives can be the same size.

NOTE: Logiccube has split the Dossier firmware into multiple files in order to optimize performance. This requires a short 45-60 second reconfiguration process that will occur when the user is switching between E01 mode to or from all other capture modes.

IMPORTANT NOTE: Always use a write protect/write block device when using the Destination Drive(s) outside of the Dossier tray (i.e. when attaching the Destination Drive(s) to a PC,

To perform a Mirror Capture



1. Make sure that the Source and Destination drives are attached to the unit and power is applied.
2. From the Main Screen, tap the **Settings** icon to enter the Settings menu.
3. Tap the **Capture** icon.
4. Tap the **Mode** icon and choose the configuration that is best suited for your capture session.

NOTE: See the Optional Preference Settings section of this chapter for more information on the Mode setting.

5. Scroll through the other optional preferences – Verify, On Error, Speed, Word List, and Modify List. Modify them as needed by tapping the different settings for each.

NOTE: See the Optional Preference Settings section of this chapter for more information on these preference settings.

6. Press the **START/STOP** button twice.

NOTE: If you have used E01 mode in a capture session immediately prior to this capture session the following message will appear:

“Need to reconfigure, continue?”

Tap the **YES** icon to continue. This process takes 45-60 seconds. When the Dossier finishes reconfiguring, a message will appear:

“Reconfiguration COMPLETED. Press any key to continue”.

Press any of the three buttons to the left of the touch screen to continue.

7. The following message will appear:
“Continuing will overwrite a portion of your destination drive(s). Are you sure?”. Press the **YES** button.
8. The Dossier will power up the drives then access the System CF card. The following message will appear: “Enter Log file name and press SET”

NOTE: If S1=>D1 & S2=>D2 Mode was selected, a screen will show “Enter S1 to D1 Log name and <SET>”. After a log name is entered, a second screen will show “Enter S2 to D2 Log name and <SET>”.

9. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the **SET** button when finished.
10. If the Destination drive has not been erased with the Wipe Destination Mode, the unit will ask if you wish to erase the Destination drive. Choose **YES** or **NO**. If **YES** is chosen, the unit will completely wipe the destination drive before it begins to capture data. This process adds significantly to the duration of the capture session.

NOTE: The log file will state whether or not the Destination drive has been properly erased.

11. The unit will “Mirror” Clone every readable sector from the Suspect drive to the Destination drive, whether or not it contains data.
12. After all sectors have been captured, if the destination drive was not erased, the unit will ask if you wish to erase the remainder of the Destination drive. Choose **Yes** or **No**. If **Yes** is chosen, the unit will completely wipe the rest of the destination drive.

NOTE: The log file will state whether or not the Destination drive has been properly erased.

13. If Auto Print was set to “Yes” in the Misc. menu, the user will be prompted to connect the printer and make sure that it is powered up and online. Press **SET** to print or **BACK** to skip printing.

NOTE: Please refer to “*Printing a Report*” later in this chapter for more printing options.

14. A copy of the Final Capture Report is written to the CF Drive. It is titled <Log file name>.LOG. The report can be accessed and printed from Windows, if the Dossier unit is connected to a PC via USB or FireWire (1394).

NOTE: Please refer to **Chapter 6: USB and FireWire Ports** for more information.

15. The capture ends with a “Capture Successful” message. It also displays the SHA-256 and MD5 Hash values for the Source and Destination drives together when the Verify setting is set to HASH + V.

IMPORTANT NOTE: Always use a write protect/write block device when using the Destination Drive(s) outside of the Dossier tray (i.e. when attaching the Destination Drive(s) to a PC,

To Perform a DD Image Capture



1. Make sure that the Source and Destination drives are attached to the unit and power is applied.
2. From the Main Screen, tap the **Settings** icon.
3. Tap the **DD Image** icon.
4. Tap the **Mode** icon and choose the configuration that is best suited for your capture session.

NOTE: See the [Optional Preference Settings](#) section of this chapter for more information on the Mode setting.

5. Scroll through the other optional preferences – [Verify](#), [File Size](#), [On Error](#), [Speed](#), [Word List](#), and [Modify List](#). Modify them as needed by tapping the different settings for each.

NOTE: See the [Optional Preference Settings](#) section of this chapter for more information on these preference settings.

6. Press the **START/STOP** button twice.

NOTE: If you have used E01 mode in a capture session immediately prior to this capture session the following message will appear:

“Need to reconfigure, continue?”

Tap the **YES** icon to continue. This process takes 45-60 seconds. When the Dossier finishes reconfiguring, a message will appear:

“Reconfiguration COMPLETED. Press any key to continue”.

Press any of the three buttons to the left of the touch screen to continue.

7. The following message will appear:
“Continuing will overwrite a portion of your destination drive(s). Are you sure?” Press **Yes**.

NOTE: The Destination drive needs to be formatted before data capture is possible. If it hasn't been formatted yet, or if the drive format is different from the saved setting (FAT32 vs. NTFS), a prompt will come up. Tap **YES** to format the drive. A confirmation prompt will appear confirming that you want to continue. Tap **YES** to begin formatting the Destination drive.

See **Chapter 4: Other Modes** for more information on managing the Destination drive.

8. The next screen prompts you to enter a Case file name using the keypad. For a DD Capture, the character limit is 195 characters except when using Spanning mode (S1 => D1 + D2) which has a character limit of 193 characters.

NOTE: If a Case file already exists on the destination drive (i.e. from a previous DD Image capture) the unit will not allow you to enter the same file name again.

9. A sub-directory (by the same name) will be created under the root directory on the destination drive.
10. The capturing process will create as many files as necessary within this sub-directory, with increasing extension numbers (e.g. my_disk.001, my_disk.002, etc.)
11. At the end of the process, a file with the **.log** extension is created and placed in the same sub-directory. The file is also written to the internal Flash memory. It includes (among other things), the SHA-256 and MD5 Hash values of all captured DD files or the entire Source Drive. Refer to the **Special Settings** section later in this chapter.
12. If Auto Print was set to "Yes" in the Misc. menu, you will be prompted to connect the printer and make sure that it is powered up and online. Press SET to print or BACK to skip printing.

NOTE: Please refer to the "*Printing a Report*" section later in this chapter for more printing options.

13. The capture ends with a "DD Capture Successful!" message. It also displays the SHA-256 and MD5 Hash values for the Source and Destination drives together when **Verify** setting is set to **Disk** or **Disk + V**.

IMPORTANT NOTE: Always use a write protect/write block device when using the Destination Drive(s) outside of the Dossier tray (i.e. when attaching the Destination Drive(s) to a PC,

Special Settings for DD Image Mode

The settings below are unique to DD Capture mode:

Verify Disk or File



For DD Image Capture Mode, the Verify Setting has some optional settings which are not available in any other mode. The settings available are:

File - This is the default setting for verification and uses special hardware to compute SHA-256 and MD5 values for each individual DD Image file.

File + V - This setting behaves like File, except that it also reads back captured data and compares it to the Source drive.

Disk - This setting uses special hardware to compute the SHA-256 and MD5 values for the entire Source drive.

Disk + V - This setting behaves like Disk, except that it also reads back captured data and compares it to the Source drive.

File Size



This setting allows the user to choose the size of captured DD Image files. The choices are:

650MB – Image files of this size can be archived on a CD-ROM.

2GB – Image files of this size can be archived on Flash Memory cards or Thumb Drives.

4GB – Image files of this size can be archived on larger Flash memory / USB drives or a DVD-ROM.

DRIVE – This selection will create a single DD image file. The size of the file depends on the size of the Source drive captured.

Loading DD Image files into a Forensic Investigative Tool

Once the DD Image files are captured to a Destination drive, they can be easily loaded into a Forensic Investigative tool that supports DD Images. Consult your software's manual for more information.

1. Attach the Dossier to the PC via the USB or FireWire Port, (please refer to **Chapter 6. USB and FireWire Ports**).
2. Load the DD Image into your software as per the Manufacturer's instructions.

NOTE: If there is an option for the number of “Bytes per sector”, set it to 512. Also, some software may ask to mount a drive as either “physical” or “logical”. If your software gives you this option, select “physical”.

E01 Image



The E01 option captures hard disk drives directly into the E01 format. The evidence or destination drive can then be easily uploaded to the analysis software in a ready-to-analyze state. This eliminates the time-consuming conversion step that users typically must perform.

E01 NOTES:

- E01 is supported from SW release 1.17 and firmware release 8.15 forward. If you need to update software and firmware to this revision in order to install the E01 option and your units S/N is below #77750 you must reset Dossier to factory default settings by pressing Misc., Manage Settings and this icon.



- At this time, the E01 Image format is supported with Encase v6.x and Forensic Toolkit (FTK) v3.x.
- E01 does not currently support captures from RAID pairs.
- Currently E01 Flash media captures can only be performed with an external flash media adapter used in conjunction with a USB enabled (Optional) SAS or SCSI adapter.

To Perform an E01 Image Capture

1. Make sure that the Source and Destination drives are attached to the unit and power is applied.
2. From the Main Screen, tap the **Settings** icon.
3. Tap the **E01 Image** icon.



4. Tap the **Mode** icon and choose the configuration that is best suited for your capture session.

NOTE: See the **Special Settings for E01 Image Mode** section of this chapter for more information on these preference settings.

5. Scroll through the other optional preferences – Verify, and On Error. Modify them as needed by tapping the different settings for each.

NOTE: See the **Special Settings for E01 Image Mode** section of this chapter for more information on these preference settings.

6. Tap the **Setting** icon to go to the E01 Setting Menu.
7. Ensure the correct (UTC) offset value is entered into the Forensic Dossier by tapping the Time Zone icon.



8. Input a value (-12~12) with the keypad to set your time zone relative to (UTC) and press the **SET** button to enter the value. Example: The UTC for Los Angeles California is UTC-8.

NOTE: To enter a negative (UTC) value:

- a. Press **Shift** then **0**.
 - b. Press **Shift** then the number.
9. To enter any notes or to select the Info Show icon press D1 or D2 respectively.
 10. Press the **START/STOP** button twice.

NOTE: If you have used a mode other than E01 in a capture session immediately prior to this capture session the following message will appear:

“Need to reconfigure, continue?”

Tap the **YES** icon to continue. The process takes 45-60 seconds. When the Dossier finishes reconfiguring, a message will appear:

“Reconfiguration COMPLETED. Press any key to continue”.

Press any of the three buttons to the left of the touch screen to continue.

11. The following message will appear:
“Continuing will overwrite a portion of your destination drive(s). Are you sure?” Press **Yes**.

NOTE: The Destination drive needs to be formatted before data capture is possible. If it hasn't been formatted yet, or if the drive

format is different from the saved setting (FAT32 vs. NTFS), a prompt will come up. Tap **YES** to format the drive. A confirmation prompt will appear confirming that you want to continue. Tap **YES** to begin formatting the Destination drive.

See **Chapter 4: Other Modes** for more information on managing the Destination drive.

12. The next screen prompts you to enter a Case file name using the keypad. For an E01 Image Capture, the character limit is 195 characters except when using Spanning mode (S1 => D1 + D2) which has a character limit of 193 characters.

NOTE: If a Case file already exists on the destination drive (i.e. from a previous E01 Image capture) the unit will not allow you to enter the same file name again.

13. A sub-directory (by the same name) will be created under the root directory on the destination drive.
14. The capturing process will create as many files as necessary within this sub-directory, with increasing extension numbers (e.g. my_disk.e01, my_disk.e02, etc.)
15. At the end of the process, a file with the **.log** extension is created and placed in the same sub-directory. The file is also written to the internal Flash memory. It includes (among other things) the MD5 Hash values of all captured E01 Image files.
16. If Auto Print was set to "Yes" in the Misc. menu, you will be prompted to connect the printer and make sure that it is powered up and online. Press SET to print or BACK to skip printing.

NOTE: Please refer to the "*Printing a Report*" section later in this chapter for more printing options.

17. The capture ends with an "E01 Capture Successful!" message. It also displays the MD5 Hash values for the Source and Destination drives together when **Verify** setting is set to **Disk** or **Disk + V**.

IMPORTANT NOTE: Always use a write protect/write block device when using the Destination Drive(s) outside of the Dossier tray (i.e. when attaching the Destination Drive(s) to a PC,

Special Settings for E01 Image Mode

The E01 selection choices for the settings Mode, Speed, Verify and On Error are different from the other modes. The selection choices are as follows:

Mode		S1=>D1 (Default)
		S1=>D1 & S2=>D2
		S1=>D1&D2
		S1=>D1+D2
Speed		Select UDMA-5 or UDMA-4 (Default is UDMA-5)
Verify		Select DISK or DISK+V
On Error Retry		Select Retry or Abort

The remaining icons are specific to E01 and are explained below.

Segment Size		Select 1500M Byte or 4000M Byte
Compression		Select YES or NO
Setting		The Settings icon is used to add relevant case information using the keypad and must be entered for the capture to initiate: Case Number Examiner Time information (yyyy/mm/dd hh:mm)
Notes		Press the Notes icon to enter up to 64 characters of pertinent information using the keypad.

Press the **SET** button to save a note. Press the **BACK** button to leave the screen without saving a note.

Info Show

Pressing the Info Show icon will display the current case information that will be tied to the E01 capture report.

Sample E01 Info

Case No: GFK008

Examiner: R_SMITH

Notes: Any notes you wish to add.

Timestamp: 200910141439

TimeZone: UTC-8

Printing a report

At completion of a capture, you might want to print a report. You must keep the Forensic Dossier powered on in order for it to retain the report information from the last session.

NOTE: Logiccube Dossier Forensic Kits purchased and shipped prior to October 14, 2009 included a Brother MW-120 portable thermal printer. This printer is also available to purchase from Logiccube.

Printing with the Brother (thermal) Printer

1. Connect the Brother printer to the Dossier using the special serial cable included with the kit.
2. Power the printer using the printer power adapter.

CAUTION: Don't confuse this power adapter with the Dossier power adapter. Press the power button on the printer until it lights up.

3. Make sure that the Brother printer is loaded with A7 size thermal paper. For paper loading instructions, refer to the Brother printer User Manual.

NOTE: Do not use plain paper in the Brother printer.

4. From the Dossier main screen, tap the **Misc** icon, then tap the **Print Options** icon.

5. Tap the **Print Reports** icon, and then tap the **Print Last Session** icon.
6. Follow the instructions on the screen. A report should now print.

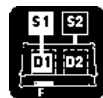
Every operation performed with the Dossier also writes a copy of the report to the CF Drive. This report can be easily accessed in Windows and printed from a text editor like Notepad.

Optional Preference Settings

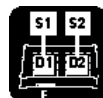
All of the preference settings below are available for Mirror Capture and DD Image Capture modes. For E01 preferences, please see the section “**Special Settings for E01 Image Mode**” earlier in this chapter.

Mode

The Mode option allows the Dossier to be configured to clone from 1 or 2 Source drives or flash media to 1 or 2 Destination drives.



S1 (Source 1) to D1 (Destination 1) – This mode allows one Source drive to be captured to one Destination drive. This is the default mode setting.



S1 to D1 & S2 (Source 2) to D2 (Destination 2) – This mode allows two separate Source drives to be captured to two separate destination drives.



S1 to D1 and D2 – This captures the contents of one Source drive to two Destination drives. This is ideal for making a copy to keep in evidence and an extra copy for investigation.



RAID to D1 – This mode allows most common RAID configurations to be copied to a single Destination drive. Please refer to **Chapter 5 – Capturing RAID Configurations**.



RAID to D1 and D2 – This mode allows most common RAID configurations to be copied to two Destination drives simultaneously. Please refer to **Chapter 5 – Capturing RAID Configurations**.



Flash to D1 – This mode is used to copy a Flash Memory card from one of the Dossier’s card slots to a single Destination drive.

NOTE: This mode automatically sets the capture speed to PIO-AUTO.



Flash to D1 and D2 – This mode is used to copy a Flash Memory card from one of the Dossier's card slots to both Destination drives simultaneously.

NOTE: This mode automatically sets the capture speed to PIO-AUTO.



S1 to D1 + D2 – This image Spanning mode is available only under DD image capture and E01 image capture. This mode allows you to capture from one large suspect drive and span DD or E01 images to two smaller evidence drives. Any subsequent DD or E01 capture performed using this mode will be added provided drive space is available. Case data is not overwritten.

NOTE: A very fast free space check enhancement has been incorporated into the latest software and firmware release. Check your Dossier frequently to ensure you benefit from these enhancements.

Verify



The Verify option is provided to add an increased level of confidence in the capture process. The choices are: **HASH**, **HASH + V** and **NONE**.

HASH – This setting uses special hardware to compute 256-bit SHA-256 and 128-bit MD5 values at an extremely fast and accurate rate.

HASH + V – This setting behaves like **HASH**, except that it also reads back captured data and compares it to the Source drive in 50MB chunks. This setting is recommended to ensure the accuracy of the hash values.

NOTE: The “+ V” settings will double the cloning time of a capture session.

NONE – No verification. This setting is only recommended for non-Forensic cloning operations.

NOTE: Without verification, bad or weak sectors on the Destination drive will not be detected. This could cause the copy to be invalid.

NOTE: When a DD capture is performed with Verify the Destination Hash Value is reported in the verify section of the audit trail report.

Speed



The speed setting provides the option to set the speed at which an operation will be performed at.

UDMA-6 – The software performs a test procedure to determine the fastest setting that the drives will tolerate while streaming data from one to the other.

When set to UDMA-6, all speeds grades below will be tested (i.e. UDMA 0-6, PIO-AUTO PIO-PIO Medium and PIO-SLOW).

UDMA-5 – With UDMA-5 selected, the software performs a test to determine the fastest speed setting that the drives will tolerate while streaming data from one drive to another.

When set to UDMA-5, all lower speed grades will be tested (i.e. UDMA 0-4, PIO-AUTO PIO-PIO Medium and PIO-SLOW)

UDMA-4 – Force the unit to use at most this speed. Set the unit to this mode in some rare situations where one or both drives do not support the higher speeds, and “misbehave” during our automatic speed benchmarking.

UDMA-3 – Same as **UDMA-4**.

UDMA-2 – Same as **UDMA-4**.

UDMA-1 – Same as **UDMA-4**.

UDMA-0 – Same as **UDMA-4**.

PIO-Auto (PIO-4) – Force the unit to use this as the highest speed (PIO-4). Set the unit to this mode in some rare situations where one or both drives do not support higher speeds, and “misbehave” during our automatic speed benchmarking.

NOTE: The unit will automatically choose this speed when capturing data from flash memory cards.

PIO-Medium – This is a fixed value that almost all drives will tolerate. It will result in copying speeds from about 200 to over 500 MB per minute depending upon the characteristics of the drives.

PIO-Slow – This is a speed value that all drives will be able to tolerate. It supports copying speeds from 100 to over 300 MB per minute depending on the characteristics of the drives.

NOTE: Use the MEDIUM or SLOW modes if you encounter drive “time-outs” or if you are capturing older drives. Many older 2.5” notebook drives require the PIO-SLOW setting.

On Error



The On Error setting determines the behavior of the unit in the case where bad spots are detected on the source (suspect) drive. This setting has four options, which include:

Skip – This is the default setting. Skip will allow the Dossier to continue by stepping over the bad sector.

Abort – This mode will cause the Dossier to halt if an error such as a bad suspect drive sector is encountered.

Retry – Retry will instruct the Dossier to make several attempts to read data from the damaged area of the drive. The user can configure the number of retry attempts from 0 to 1000 by pressing the Retries icon under Misc. to set the desired value.

Recover – Recover will attempt to recover as many bytes of data as possible from each bad sector that is encountered

NOTE: Data in any skipped sectors will NOT be copied to the destination drive. The corresponding sector of the Destination drive will instead be “padded” with zeroes. The padded sector will then be included in the final SHA-256 and MD5 values.

ADDITIONAL NOTE: The absolute location of each skipped sector will also be listed on the final Capture Report. The first 200 bad sectors will be recorded, after which the unit will continue to skip bad sectors but it will not record their absolute locations. The final capture report will show the total number of sectors skipped.

Option	Action	Time to complete
Abort	A bad sector aborts the cloning operation	Immediate
Skip (default)	Skips the bad sector	Fast
Retry	Attempts several retries to recover data of sector, then skips	Slower
Recover	Attempts a full-blown recovery algorithm, then skips	Very slow

Table 1, Error settings

Note: When capturing a Source drive that is known to have many bad sectors, the speed should be set to PIO-AUTO. Also, if the drive is captured or scanned multiple times, the SHA-256/MD5 Hash value of each session could differ. This is because some bad sectors will read intermittently.

Word List



The Word List Option is described in more detail in **Chapter 7: Keyword Searching**.

Modify List



The Modify List Option is described in more detail in **Chapter 7: Keyword Searching**.

Capturing Data from HPA and DCO Configurations

Some PC manufacturers will employ a utility that creates a HPA or DCO configuration on a hard drive. These configurations are designed to change drive characteristics such as drive capacity, speed and other settings as they are reported to the PC BIOS.

HPA – Or Host Protected Area can limit the size of a hard drive, but it can also change many other settings such as speed and S.M.A.R.T. status.

DCO – Or Device Configuration Overlay limits the size of a drive only. For example, a 60GB drive can be made to look like a 30GB drive to a PC.

The Dossier is able to unlock and capture data from both HPA and DCO configurations. The Dossier will then re-lock the DCO. HPA's are relocked when the Source drive is hard-booted after capture.

The Final capture report is also able to report any HPA and/or DCO that is found.

The report only shows the existence of an HPA and if it was unlocked.

The report also shows the existence of a DCO and if it was unlocked and captured. It also lists the maximum LBA, size and speed setting of the DCO

HPA and DCO configurations can only be detected on the Source drive. They cannot be seen on the Destination drive. The following Modes are able to detect, unlock and work with data inside HPA and DCO configurations when the drive is in the Source position:

- Drive Info
- Capture
- DD Image Capture
- Drive Defect Scan
- Calc. HASH
- Keyword Search

4. Other Modes

Introduction

This chapter discusses other options that are found in the Settings menu. They are **Drive Defect Scan**, **Wipeclean™ Destination** and **HASH Scan**. This chapter also discusses the options in the **Misc Menu** accessible from the Main Screen.

NOTE: **Keyword Search** and related settings are discussed in **Chapter 7** and **USB/FireWire Mode** is discussed in **Chapter 6**.

Settings Menu Options

Drive Defect Scan



This function performs a surface scan of the drive media using the drive controller to verify the media. It is designed to look for bad sectors, weak sectors or weak spots, which it reports at the end of the scan.

Procedure



1. From the Main Screen, tap the Settings icon.
2. Tap the Drive Defect Scan icon.
3. Tap the “Drives” icon. Choose one of the following drives: S1, S2, D1, D2 or Flash. Press the Set button to confirm.
4. Tap the “Speed” icon. Here you have two choices:
 - **FAST** (default): This mode does a single surface scan of the drive.
 - **SLOW**: This mode performs three surface scans in a row to better check for bad or weak sectors.
5. Press the **START/STOP** button to start the scan.

6. The Dossier will access internal flash memory, then the following message will appear: "KEYPAD ENTRY: Enter Log file name. Press Set when done".
7. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the Set button when finished.
8. When finished scanning, the Dossier will display the number of bad or weak sectors found on the drive. A copy of the session report will also be copied to the internal flash memory as <Log file name>.LOG.
9. If the Printer was set to "Auto Print", the user will be prompted to connect the printer and make sure that it is powered up and online. Choose YES to print or NO to skip printing.

NOTE: Please refer to **Chapter 3. Drive Capture Modes and Settings** for more printing options.

Wipe Destination



This function is the process that erases or wipes all existing information from the surface of the Destination drive. It is a good idea to erase the drive prior to performing Mirror captures. It ensures that no old data remains on the drive, to be later confused as evidence. Note; information regarding performing a wipe to DoD specifications can be found in the Other Settings section under Manage Destination.

Many newer drives will also support **Security Erase Mode**, which is a much more automated process for wiping data. This mode sends "Security AT" commands to the Destination drive, which allows it to wipe at a very high rate of speed. The unit will automatically switch to Security Erase if it is supported by the attached drives.

NOTE: Security Erase will not run as part of a Mirror Capture session. Ordinary Wipeclean mode is used instead.

Procedure

1. From the Main Screen, tap the Settings icon to enter the Settings menu.
2. Tap the Wipe Destination icon.
3. Tap the "Drives" icon. Choose one of the following: D1, D2 or D1 & D2 to wipe both drives simultaneously.





4. Tap the “Speed” icon to set the desired UDMA or PIO speed.
 5. Set the Signature setting to the desired position, there are two choices:
 - **YES** (Default): Writes a small signature to the drive every 16,065 sectors (or every logical cylinder). During a later capture session, this signature tells the Dossier that the drive(s) have been correctly erased.
 - **NO**: Leaves the signature off the drive. The Dossier will not detect that the drive has been erased.
 6. Press the <Start/Stop> button to begin wiping.
 7. The Dossier will access internal flash memory, then the following message will appear: “KEYPAD ENTRY: Enter Log file name. Press Set when done”.
 8. Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the Set button when finished.
 9. The Dossier will automatically detect whether or not the Destination drive will support a Security Erase. If not, then the Dossier will perform an ordinary Wipeclean operation based on the settings chosen by the user.
- NOTE:** Just before the wipe starts you may see a message on the UI that says “Set Dest PW to Spaces” This means that a Password key command has been sent to retrieve the security erase support status of the destination drive. No user action is required. If the Dossier performs a Security Erase, it will do a rough estimate of the Time Remaining. This estimate will appear on the progress bar while an “Elapsed Time” counter will count up the actual erase time.
- NOTE:** The Progress bar will appear to “hang” at 99% if the actual erase time is longer than the estimated time. The elapsed time counter will continue to run and the Status light will keep blinking until the wipe is finished.
10. When finished, the Dossier will display the following message “drive successfully erased”. A copy of the session report will also be copied to the internal flash memory as <Log file name>.LOG.

NOTE: The operation will abort with an error message if bad sectors are encountered on the Destination drive.

11. If the Printer was set to “Auto Print”, the user will be prompted to connect the printer and make sure that it is powered up and online. Choose YES to print or NO to skip printing.

NOTE: Please refer to **Chapter 3. Drive Capture Modes and Settings** for more printing options.

HASH Scan



This mode computes the SHA-256 and MD5 Hash values for a given drive (S1, S2, D1, D2 or Flash). It can also scan individual files (on the Destination Drive).

Procedure

1. From the Main Screen, tap the Settings icon to enter the Settings menu.
2. Tap the Hash Scan icon.
3. Tap the “Drives” icon. Choose one of the following drives: S1, S2, D1, D2, Flash, File on D1 or File on D2.
4. Tap the “Speed” icon to set the desired UDMA or PIO speed.
5. If a certain number of sectors need to be scanned, go to the “Size” setting. Use the keypad to enter a size in number of sectors. Press the Set button to confirm.
6. Press the <START/STOP> button to begin the scan.
7. The Dossier will access the CF Drive, then the following message will appear:
“KEYPAD ENTRY: Use the alphanumeric keypad to enter a Log file name of 8 characters or less. Press the Select button when finished.

NOTE: The operation will abort with an error if bad sectors are found on the drive.

8. When finished, the Dossier will display the SHA-256 and MD5 Hash values. A copy of the session report will also be copied to the CF drive as <Log file name>.LOG.



9. If the Printer was set to “Yes”, the user will be prompted to connect the printer and make sure that it is powered up and online. Press SELECT to print or BACK to skip printing.

NOTE: Please refer to **Chapter3. Drive Capture Modes and Settings** for more printing options.

Misc Menu Settings



This section describes the settings that are available under the **Misc Menu** that can be accessed from the Main Screen.

Backlight



Use this setting to turn the Touch Screen’s backlight on and off. This setting is useful for seeing the Touch Screen in low light conditions. The default setting is OFF.

Authenticate Trail



This mode is used to verify the authenticity of a report that has been written to the internal flash memory. It is designed to check the report for alteration. It verifies a proprietary Hash value that is written to the end of each report at the time of creation.

Procedure

1. From the Main Screen, tap the Misc icon.
2. Tap the Authenticate Trail icon.
3. The Dossier will display a list of the Log files that are on the internal flash memory.
4. Tap the desired Log file and press OK.
5. If the report has not been altered, the message will read “Log file authenticated. Press any key to return”.
6. If the report has been altered in any way, the message will read “Log File not authenticated. Press any key to return”.

7. Press the Back icon to return to the Main Screen.

Manage Setting



This icon brings up a series of icons that allow you to adjust, save and reset various default settings.

Contrast



Use this setting along with the two Up Down arrow icons to increase or decrease the Touch Screen's Contrast setting to your desired preference. The contrast setting will be retained in memory by pressing the OK icon.

Save Settings



Use this icon to save current configuration settings. Settings that can be saved through power recycle are: Mode, Speed, Verify, On Error, Contrast, Wipe Signature ON/OFF and Defect Scan Speed Fast or Slow.

Factory Settings



Changes all adjustable settings to the default factory settings.

Manage Destination



This menu is used to prep the Destination drive(s) prior to running a DD Image or E01 Image capture. The settings available are:



Format D1 – This function formats the drive in the D1 position with a single partition using the NTFS or FAT32 file system extremely quickly with the latest firmware release. This is necessary before DD Image files or E01 Image files can be copied to the drive.



Format D2 – This function formats the drive in the D2 position with a single partition using the NTFS or FAT32 file system



extremely quickly with the latest firmware release. This is necessary before DD Image files or E01 Image files can be copied to the drive.

Format – This function allows you to select the type of formatting to be performed on the Destination Drive(s). The two choices are:

NTFS – This formats the drive(s) with a single partition using the NT File System (NTFS).

FAT32 – This formats the drive(s) with a single partition using the FAT32 file system.

When Format D1 or Format D2 is activated, the following prompt appears:

“Reformatting the Drive! All data on your Internal Drive will be lost! Continue?”

Choose <Yes>, the display will say “Zeroing first FAT” and “Zeroing second FAT” as it formats the drive. After 30 – 60 seconds the drive(s) will be formatted, (the time varies by drive size).

Choose <No>, the display will then go back to the Format Dest. menu.



Scan Disk – This function checks the Destination Drive for proper formatting. It also makes sure that the FAT32 partition is not corrupt. It functions much like Microsoft Windows Scandisk or Chkdsk.

Choose <Yes> to run Scan disk. After 30 seconds, it will display a list of errors, if any.



DoD Wipe – In compliance with DoD M-5220, the Dossier will wipe either destination as follows: The drive will be wiped with all 0's followed by all 1's THREE consecutive times; after this the final value of 0xF6 will be written to all locations on the drive. To summarize, the Dossier will write the following 7 patterns to all the locations on the destination drive: all 0's, all 1's, all 0's, all 1's, all 0's, all 1's, 0xF6

DoD Wipe is located under Misc. and Manager Destination icon. Once pressed you will be asked to select between DoD Wipe D1, DoD Wipe D2 or DoD Wipe D1 & D2.



Browse Dest. – If the Destination drive is formatted with a FAT32 partition, Browse Destination will allow the user to navigate directories on the drive. It will also show the size of files on the drive. Use the Arrow and Select icon to navigate the directories.

Print Options



This mode is used to print reports directly from the Dossier through the serial port. This menu is used to prep the Destination drive(s) prior to running a DD Image capture. The settings available are:

Eject Page



This function sends a form feed signal to the printer. This function may be required to load paper in some printers.

Print Report



This function is used to manually print a report after a capture session. It also prints different reports associated with Keyword Search.



Print Last Session – This function prints the report from the last performed session (drive capture, defect scan, wipe, etc.). It is not able to print reports prior to the last session.



Print Search Detail – This function prints all of the found keywords from the last keyword search as well as their absolute locations on the Source drive.

NOTE: For more information, please refer to **Chapter 7: Keyword Searching**.



Print Search Text – This function prints a fragment of text before and after each found keyword. This allows each keyword to be viewed in context.

NOTE: For more information, please refer to **Chapter 7: Keyword Searching**.

Auto Print (After Capture)



This function tells the Dossier to print a report after the next capture session. It can be set to YES or NO (default).

Debug



Use this setting to turn the Debug reporting tool on and off. This setting is used in conjunction with Serial Port 2 and a terminal link program. The default setting is OFF. Debug should only be turned on when the user is directed to do so by Logicube Technical Support.

Beeper



Use this setting to turn the beeper on and off. This setting is useful when in “stealth” mode or in an environment that requires no noise. The default setting is OFF. Any change to the setting is preserved after power off.

Audio Notice for Error



Use this setting to provide an audible beep if the data capture has been completed successfully. A different audible beep will occur to alert the user that the capture has encountered an error. This beep will sound with a 50% duty cycle for approximately 2 minutes or until the user acknowledges the error via the user interface. The default setting for Audio Notice is OFF. Once enabled the Dossier will retain the setting last used prior to power recycle.

Security



This feature provides the user with a password-based security system (based on the ATA security specification T13) to protect their data from unauthorized access.

This feature has two security levels; **High** or **Maximum** and the ability to set a **Master** along with a **User** password. The **Master** password is typically used by an administrator – this password is kept secret from the user and may be used to unlock the device if the **User** password is lost. If **High** security is selected the drive can be

unlocked for use with either the **User** or **Master** password. Under **Maximum** security mode the drive can only be unlocked with the **User** password.

Note: Not all hard drive models support the Secure Lock function. Make sure the drives you are using support the ATA lock command. See the **Get Security Level** feature defined below for information on how to determine if a particular drive supports the ATA lock command.

The security system is enabled by sending a user password to the device. When the security system is enabled, access to user data on the drive is denied after a power cycle until the User password is sent to the device with the Unlock command.

Note: Passwords should be limited to 16 characters or less. Password entry confirmation has been implemented.

WARNING! Please be very careful when entering passwords so you are not inadvertently locked out of any drives permanently.

The security menu is accessed from the Preferences Settings Menu under Misc. (Press the "More" button to see the Security icon). The Security menu contains the following options:

High Security



When selected the drive can be set to lock with **User** and then the **Master** password. In High security mode, the **Master** password should be entered after the **User** password.

Maximum Security



This security setting can only be set to lock by the **User** password.

Type



This setting determines which user is currently accessing the drive and which password will be used to lock/unlock the drive. The choices are **Master** or **User**.



If **Master** password is selected ;



Set Password

When selected, the user is prompted to select the location of the hard disk drive that will be locked, either S1, S2, D1 or D2. Next the user will be prompted to enter the password to be assigned. Passwords can be alphanumeric, are case sensitive and should be limited to 16 characters or less. The user will be asked to enter the password a second time and once the operation has been completed the user will see the following message:

*Setting drive (XX) **Master** password is successful!*



Unlock Password

When selected, the user is prompted to select the location of the hard disk drive to unlock, either S1, S2, D1 or D2. Next the user will be prompted to enter the password to unlock the drive. When the operation has been completed the user will see the following message:

*Unlocking drive (XX) **Master** password is successful!*

Note: This unlock is temporary and the user can access the drive only once. The password will need to be reentered every time you want access to the drive even if you don't cycle the power of the Dossier.

If **User** password is selected ;



Set Password

When selected, the user is prompted to select the location of the hard disk drive that will be locked, either S1, S2, D1 or D2. Next the user will be prompted to enter the password to be assigned. Passwords can be alphanumeric, are case sensitive and should be limited to 16 characters or less. The user will be asked to enter the password a second time and once the operation has been completed the user will see the following message:

*Setting drive (XX) **User** password is successful!*



Unlock Password

When selected, the user is prompted to select the location of the hard disk drive to unlock, either S1, S2, D1 or D2. Next the user will be prompted to enter the password to unlock the drive. When the operation has been completed the user will see the following message:

*Unlocking drive (XX) **User** password is successful!*

Note: This unlock is temporary and the user can access the drive only once. The password will need to be reentered every time you want access to the drive even if you don't cycle the power of the Dossier.

Get



To initialize the **Get** update the user must recycle system power after any setting change. **Get** will access hard disk drive security information for one user selectable drive; S1, S2, D1 or D2. The feature reports the security settings that are implemented on the selected drive. For example;

Security supported	Yes
Security enabled	Yes
Security locked	Yes
Security frozen	Yes
Count expired	Yes
Security level	High

Disabled



This option will permanently remove any previous security feature passwords from the hard disk drive, allowing anyone access to the drive even after drive power is recycled. Users can select one drive at a time to disable, either S1, S2, D1, D2. In high security mode the security feature can be disabled using either the **User** or **Master** password.

SCSI/SAS Adapter



The SCSI and SAS Adapters are designed to attach directly to the Logicube Forensic Dossier. These optional adapters can be purchased from Logicube. Contact the Logicube Sales Department for more information.

Functionally each adapter acts like a pass through device and allows for external connection and capture of SCSI and or SAS source drives through the IDE port of Dossier.



Info is used to display the Serial Number and current Firmware, BIOS, Kernel and Software revisions for the SCSI or SAS adapter you have connected to the source position of Dossier.



BIOS Upgrade is used to upgrade the BIOS of the adapters PCB assembly.



Kernel Upgrade is used to upgrade the OS of the adapter.



FPGA Upgrade is used to upgrade the Firmware of the adapters PCB assembly.



The Application Upgrade icon is used to upgrade the Capture Application for both the SCSI and SAS adapters. This update will most likely to be performed more frequently than those listed above.

Performing SAS and SCSI Adapter Updates

It's good practice to occasionally verify that your Adapter is running the current BIOS, Kernel, Firmware and Software Application. This is not something that will need to be updated frequently.

The Application Upgrade icon is used to upgrade the Capture Application for the both adapters. This update will most likely to be performed more frequently than those listed above.

Press the following icons in succession to display a list of the current programming installed in the attached adapter:

Misc. mon 

A list will display showing which version of BIOS, Kernel, FPGA (Firmware) and Application Software currently installed in the adapter.

Sample Info list:

Serial number: 1
Firmware Rev: 101
Bios Rev: 150
Kernel Rev: 200
Software Rev: 302

Compare the versions in your list to the current versions posted and available on the Logicube website. If updates are necessary download the files that need updating from www.logicube.com/support Select product F-ADP-SAS or F-ADP-SCSI and the applicable download links will be visible. The downloads are in ZIP format. Unzip the contents to the root directory of a USB flash drive then follow the update instructions starting at step 1 below.

NOTE: The USB port on the adapter is used to update all Adapter programming even if the USB port cloning option has not been purchased and enabled.

The following are Step-by-Step instructions on how to update Adapter BIOS using the Forensic Dossier. Kernel, FPGA and Software are updated similarly.

1. Disconnect the power supply cord from the Logicube Hard Disk Drive capture device.
2. Locate the IDE ribbon cable P/N CBL-037B and plug the end labeled HDD SIDE into the adapter port marked IDE CONNECTOR IN.
3. Connect the other side of the ribbon cable labeled DUPLICATOR SIDE to an external IDE port on the Logicube capture device you are using.

4. Locate the cable labeled CBL-002B and connect the end with the large white plug to the mating receptacle next to the IDE ribbon cable on the adapter.
5. Connect the other side of the CBL-002B to the external power port of the Logicube capture device. Use the power port closest to the ribbon cable.
6. Copying the files to be updated to the root directory of a USB flash drive. Updated files are located at www.logicube.com/support Select product F-ADP-SAS or F-ADP-SCSI and the download links will be visible.
7. Insert the USB flash drive into the adapter USB port.
8. Insert the power supply cord to power the duplication device.

NOTE: The remaining steps provide instructions to update BIOS but are also applicable for updating Firmware, Kernel and Software.

9. Press **Misc. m**  
10. Enter the password [logicube] in lower case.
11. You will be prompted to enter a revision number. If this example it is the current BIOS revision number. This and all current revision numbers are provided in the readme.txt file that accompanied the previously downloaded update files. As of this writing the value for Bios Revision is 150. Entering an incorrect revision value will cause the process to error out.
12. Enter the current revision for the respective item you are updating. If the revision number matches the excepted number the update process will begin.

NOTE: It is imperative that power be maintained throughout the SAS adapter update.

NOTE: Please refer to **Section 8: Optional Peripherals** for information regarding use of the optional SCSI/SAS adapters.

Retry



Use this setting to set the number of “read/write error” retry attempts from 0 to 1,000. Use the keypad on the Dossier to set the number. The default setting is 50.

Install Options



As optional features become available, use the install options icon to activate purchased options by pressing Misc. and the Install Options icon on Dossier.

Enter the alphanumeric option code provided at time of optional purchase using the touch screen display. The option will automatically become available.

NOTE: New and improved Dossier software will appear from time to time on our web site located at www.logicube.com. Verify your software is up to date by comparing the software revision on the Logicube website with the software revision listed under About on the main menu.

File System



This function allows you to select the file system used for Destination drives. If the file system on your Destination drive differs from this setting, you will be prompted with the following message:

“D1 File System is different from setting!
Would you like to change setting(No) or reformat(Yes)?”

The two choices for the type of formatting are:

NTFS – This formats the drive(s) with a single partition using the NT file system (NTFS). This is the default setting.

FAT32 – This formats the drive(s) with a single partition using the FAT32 file system.

Languages



This function allows English, Spanish or Chinese (simplified or Traditional) characters on the Dossier display. Each selection has an option for YES or NO.

From the Main Dossier menu, tap the **Misc** icon, then tap the **More** icon twice, and finally tap the **Languages** icon. The following choices will appear:



Simplified Chinese
(YES/NO)



Traditional Chinese
(YES/NO)



Spanish
(YES/NO)



English
(YES/NO)

Time Zone



This function allows you to set the time zone. A value from -12 to 12 can be used (UTC offset). Set this to your time zone. For example, use -08 for Pacific Time.

NOTE – For time zones with half hour increments, please see the setting for 'Daylight Saving' later in this section.

E01 Resume



This function allows you to view previously skipped incomplete sessions. When this function is selected, the Dossier will access its journal and display each previously skipped incomplete session one at a time. From this screen you can resume the incomplete session by tapping the **Res** button or skip to the next incomplete session by tapping the **Skip** button.

NOTE: When resuming an incomplete session, the same Source and Destination drive(s) must be attached to the Dossier. An

error will appear if the serial numbers of the Source or Destination drive(s) do not match.

Daylight Saving



In this section you can place an offset for daylight savings time. The format is HH:MM. For example, if you are currently observing Daylight Savings, input 01:00 to add an hour.

For time zones with half hour or quarter hour increments (for example, IST or IRST), you can input 00:30 to add 30 minutes to the time zone.

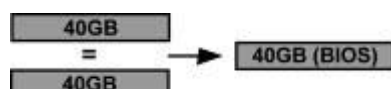
5. Capturing RAID Configurations

Introduction

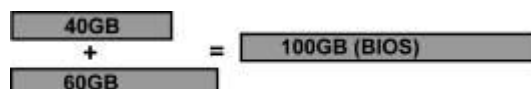
The built-in RAID I/O Feature has the ability to clone data from two separate RAID drives to a single Destination drive. This ability supports **RAID-0**, **RAID-1** and **JBOD** configurations. These configurations are described below:



- **RAID-0:** This configuration splits data evenly over two separate hard drives so that they are seen as one large drive in the PC BIOS. This configuration is also known as a **striped set**.



- **RAID-1:** This configuration creates an exact copy of one drive's data across two separate hard drives. It is designed to provide uninterrupted service should one of the hard drives go down. This configuration is also known as a **mirror**.



- **JBOD:** This configuration is able to distribute data over two drives of different size so that the drives appear in BIOS as one single drive. JBOD stands for "**Just a Bunch of Drives**".

Source Drive Cloning Notes

The following settings behave differently when a Source RAID configuration is attached to the Dossier:

Drive Capture and DD Capture

Be sure to set the Mode Setting to **RAID => D1** or **RAID => D1 and D2** before capture.

Verify

Verification cannot be set to a “+V” setting or the capture session will stop with an error message: “The current Verify setting is not supported with a RAID Source”. All other verification settings are acceptable.

Calculate HASH and Keyword Search

Calc. Hash and Keyword Search modes are not supported for RAID configurations at this time.

Other Notes

To verify the MD5 or SHA-256 Hash with a third party method, RAID Source drives must be write protected, then re-attached to their RAID controller and examined with a software-based utility (like Winhex). Connecting to different RAID controllers will produce uneven results. Also, connecting the Source drives without write-protection will change the HASH values of the Source drives. Destination drives can be scanned without the use of a RAID controller.

6. USB and FireWire Ports

Introduction



The integral USB and FireWire (1394) ports on your Logicube Dossier provide connectivity of the unit and its connected drives to any PC with active USB and/or FireWire ports. It also ensures zero alteration to Source and Destination drives under any operating system. USB 1.x and 2.0 are supported.

Additionally, drive capturing through the USB and the FireWire port is possible with the USB/FireWire Cloning Software included on a separate CD-ROM with your Dossier.

IMPORTANT NOTE: Suspect Flash drives are also write protected when Dossier is connected to a PC. The System CF, however, is not write protected. Exercise caution when connecting to the System CF card so that log reports are not deleted.

Minimum requirements

- A Logicube Dossier unit with integral USB / FireWire ports.
- A 586 or better PC compatible computer with CD-ROM drive.
- An active USB port and/or an active FireWire (1394) port.
- Microsoft Windows 98SE/ME/2000/XP/Vista/7 operating system (for drive access under Windows).

NOTE: WIN98 USB drivers can be found on the CD-ROM included with the Dossier.

- A bootable CD for DOS capturing mode, (optional).



Figure 11, USB Port on Logiccube Dossier

USB Connection to Windows (for Drive Management)



Please refer to Figure 11:

1. Make sure that the desired drive(s) are attached to the Dossier
2. Make sure your PC is running Win98 or above.
3. With power applied to Dossier connect the USB cable (provided) to a PC USB slot on one end. Do not attach the other end to the Dossier yet.
4. From the Main Screen of the Dossier, tap the Settings icon.
5. Press the USB / 1394 icon
6. Tap the USB icon, 2 settings will appear:



- **Drive:** Choose one of the following drives to connect: S1, S2, D1, D2, Flash or System CF (Dossier's internal flash memory).
7. Press Start twice and Dossier will power up the chosen drive. A prompt will appear saying "USB Link Up..."
 8. It is now safe to attach the USB cable to the Dossier. You should now see some activity on your PC screen, which depends on the operating system.
 9. If running ME/2000/XP/Vista/7 your drive will automatically be mounted and drive letters assigned to all recognizable partitions.
 10. If running 98/98SE you will be prompted to install drivers. At the "have disk..." prompt

please point the PC to the drivers floppy (provided), and the installation should complete smoothly.

11. The chosen drive is now visible on Windows as an external drive. Any partitions that can be accessed by your Operating System will be assigned a Drive Letter.

At this point the drive is fully visible to any Forensic analysis tool, such as EnCase, iLook, and FTK. The drive contents, however, cannot be altered in any way. Note that since Windows keeps caching information for every drive, some operations (such as file read), may appear to show changes in file access time etc. but these are purely virtual, and do not change anything on the drive itself.

FireWire Connection to Windows (for Drive Management)



Please refer to Figure 11:

1. Make sure that the desired drive(s) are attached to the Dossier
2. Make sure your PC is running Win98 or above.
3. With power applied to Dossier, connect the FireWire (1394) cable (provided) to a PC FireWire slot on one end. Do not attach the other end to the Dossier yet.
4. From the Main Screen of the Dossier, tap the Settings icon or press the Set button.
5. Press the USB / 1394 icon.
6. Tap the FIREWIRE IEEE 1394 icon, 2 settings will appear:



- **Drives:** Choose one of the following drives to connect: S1, S2, D1, D2, Flash or System CF (Dossier's internal flash memory).
7. Press Start twice and Dossier will power up the chosen drive. A prompt will appear saying "FireWire Link Up..."
 8. Attach the FireWire cable to the Dossier. You should now see some activity on your PC screen, which depends on the operating system.
 9. If running ME/2000/XP/Vista/7 your drive will automatically be mounted and drive letters assigned to all recognizable partitions.

10. If running 98/98SE you will be prompted to install drivers. At the "have disk..." prompt please point the PC to the drivers floppy (provided), and the installation should complete smoothly.
11. The chosen drive is now visible on Windows as an external drive. Any partitions that can be accessed by your Operating System will be assigned a Drive Letter.

At this point the drive is fully visible to any Forensic analysis tool, such as Encase, iLook, and FTK. The drive contents, however, cannot be altered in any way. Note that since Windows keeps caching information for every drive, some operations (such as file read), may appear to show changes in file access time etc. but these are purely virtual, and do not change anything on the drive itself.

Removing USB devices



Before physically disconnecting the USB cable and/or shutting down power to the Dossier, the unit has to be properly "unmounted" from Windows. To do that:

1. Locate the USB icon in the system tray (typically at the bottom right of screen).
2. Click the icon once.
3. Wait for Windows to bring up a message that it is safe to remove the device. (Different versions of windows will behave slightly differently).

Cloning through the USB/FireWire ports



This mode allows the user to clone drives through the USB or FireWire ports of a PC. The PC drive can only be the Source drive. Both USB 1.x and 2.0 and FireWire (1394) are supported. Typically, the user will boot the computer from the provided boot CD. The CD is equipped with USB and FireWire drivers and our drive capturing application.

USB/FireWire Cloning only works with one Source drive cloning to one Destination Drive (**D1**).

How to set up and use the USB/FireWire cloning software:

1. Follow these instructions to maintain the forensic integrity of the capture. With computer power off, insert the boot CD into the CD-ROM drive or, depending on the computer's CD-ROM drive you may need to insert the CD as far as it will so it can be pulled in during power up. Start the computer and immediately enter the BIOS setup menu. This varies by computer but usually requires you to press (F12, F1 for IBM or the Delete key for most generic PCs) just after startup. Make sure that the PC is set to boot from the CD-ROM as the first bootable device. Allow the PC to continue booting off of the boot CD in the CD-ROM drive.
2. The Forensic USB Cloning CD-ROM is configured to automatically load the necessary drivers and run the client application. The user will be presented with a User Interface and a menu to select among the various capture options and settings.

NOTE: A USB or FireWire connection must be made between the computer and the Logicube forensic capture device either before or after the Boot CD application starts. The following message will be displayed if the application starts without detecting connection to a Logicube forensic capture device: *Searching for Logicube Forensic Device. Make sure it is connected.*

3. On the Forensic Dossier attach a hard drive to the Destination (Internal) position that is larger than the suspect drive you intend to capture.
4. Attach a USB or FireWire cable to the PC (do not attach the other end of the cable to the Dossier yet).
5. From the Main Menu on the Forensic Dossier, tap the following icons in order:
 - a. Settings
 - b. More
 - c. USB/Firewire
 - d. USB or Firewire (which one you will use)
 - e. Drive
 - f. D1

6. Based on your previous selection, connect either the USB or FireWire cable to the Forensic Dossier and press the START/STOP button again.
7. The PC client software should now detect the presence of the Logicube Forensic Dossier you are using. The cloning software interface will then come up. All available functions will now be controlled from the PC client software application. The application will display a menu containing three columns *PC Source Drives, Partitions and Modes*.

NOTE: For DD captures only, if the destination drive is not formatted with a FAT32 partition, the application will prompt the user and will format the drive accordingly. If there is not enough room in the destination drive for a DD file capture, the application will exit with an error, notifying the user.

Selectable Capture Modes & Options

- **Native:** This is analogous to a mirror copy of the PC's internal drive to the Destination. This mode calculates and displays an MD5 Hash value.
- **Native +V:** Capture suspect drive and compute MD5 on the master drive. The destination drive is then read back, an MD5 hash is computed on it and compared with the Master hash. The Capture Utility display the Total MD5 Hash value on the screen at the end of the capture session.
- **DD-Image-650M:** The Master drive is broken up into (650 M byte files) and a MD5 hash is computed on every file. (MD5 Hash values are calculated for each DD image) This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.
- **DD-Image-650M+V:** The Master drive is broken up into (650 M byte files) and a MD5 hash is computed on every file. The destination drive is then read back, an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is

generated and saved in the destination drive at the end of the session.

- **DD-Image-2G:** The Master drive is broken up into (2 G byte files) and a MD5 hash is computed on every file. This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.
- **DD-Image-2G+V:** The Master drive is broken up into (2 G byte files) and a MD5 hash is computed on every file. The destination drive is then read back, an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.
- **DD-Image-4G:** The Master drive is broken up into (4 G byte files) and a MD5 hash is computed on every file. This requires the drive to be formatted with a FAT32 file system partition. There is a log generated and saved in the destination drive at the end of the session.
- **DD-Image-4G+V:** The Master drive is broken up into (4 G byte files) and a MD5 hash is computed on every file. The destination drive is then read back, an MD5 hash is computed on it and compared with the Master hash. This requires the drive to be formatted with a FAT32 file system partition. A log file is generated and saved in the destination drive at the end of the session.
- **Compute Source MD5:** An MD5 hash is computed on the entire internal PC drive. The resulting value is displayed on the screen.
- **Compute Destination MD5:** An MD5 hash is computed on the entire destination drive. The resulting value is displayed on the screen.
- **Erase Destination:** A single pass wipe is performed on the destination drive. For erase the Capture Utility reports Total Drive Sectors, Erased Sectors, Erase speed in MB/Minute, Time to Completion and % Complete.

8. Use the arrow keys on your host PC's keyboard to navigate through the various settings of the capture utility. Use the "Enter" key to make selections and the "S" key to start a process.
9. On the left side of the screen you will see a list of up to four available drives. Choose the "Source" drive you wish to capture by scrolling through the selections using the up/down arrow keys on your PC's keyboard. When your selection is highlighted a brief description of the drive will appear in the middle of the screen. Press "enter" to select a source drive.
10. On the right side of the screen you will see a list of capture modes. You can scroll through the selections using the up/down arrow keys on your PC's keyboard. Press "enter" to make your selection.
11. Once you have selected the "source" drive to be captured and selected the method of capture press "S" to start the data capture. A progress bar will appear on the screen.
12. You may cancel or abort the capture at any time by pressing the "Esc" key. Press any key and answer [Y]es to return to the main menu.
13. Once the capture has been completed a message will pop-up indicating the capture session has completed successfully.
14. If you have selected a capture method with an MD5 Hash the hash values will appear at the bottom of the screen.

NOTE: Except for DD captures, the hash values generated will not be saved if you exit this screen. You must record the hash values before exiting!

15. Upon completion of the data capture press any key and answer [Y]es to go back to the main screen. To perform a data capture from another source drive, install a new destination drive only if the current destination drive is full or your next capture will be performed as Native. Repeat steps 9 through 16 to perform a subsequent data capture.
16. To exit the Forensic Cloning Software, press the Esc key and answer [Y]es. A message will display that indicates "You can now remove the CD-ROM". Some computers will automatically eject the CD at this point.

Power down the PC as soon as the CD has been removed from the CD-ROM drive to maintain the forensic integrity of the capture.
Do not re-boot!

Cloning a Mac using FireWire and the Cloning Software:

Follow these instructions to maintain the forensic integrity of a HDD capture from a Mac computer. You will need a host PC (Non-Apple/Mac) with FireWire support to run the USB/FireWire cloning software. Ensure that the Mac is turned OFF.

NOTE: The MacBook Air is not supported at this time.

1. Install a FireWire cable between the host PC running the cloning software and the Apple computer to be cloned.
2. Power up the Apple computer, wait for the BIOS chime and immediately press and hold "T" to enter FireWire Target Disk Mode.
3. Load the cloning software CD onto the non-Apple/Mac PC by following instructions 1 through 8 on pages 2 - 4.
4. With FireWire Target Disk Mode already established, the User Interface on the host PC will display the Apple computer's hard drive in the list of available drives as soon as the cloning software is loaded.
5. Load the cloning software CD onto the non Apple PC by following instructions 1 - 16 above.

Additional Notes

- Capture speed depends on the USB and FireWire hardware and the processor speed of the PC. Expected capture speeds are up to 1.4GB/min with verify and up to 1.8GB/min without verify. Your capture speeds may vary.
- 400/200/100 speed FireWire ports are supported. 800 Mbps FireWire is not supported.
- Upon detection of an error the capture will skip the bad sector(s) and write zeroes to the corresponding sector(s) on the destination drive.

- During most operations the capture utility reports Total Drive Sectors Cloned, Speed in MB/Minute, Time to Completion and % Complete.
- Due to the absence of a FireWire connection MacBook Air is not compatible with the Logiccube boot CD.

7. Keyword Searching

Introduction



The Dossier unit can search for multiple keywords while capturing a suspect drive. This is a useful feature to provide early screening of a drive. For example, you could search for the names of all common drugs or the names of known offenders on a given drive. Presence of these keywords might indicate a connection between the suspect and the keywords.

In general, you select a pre-defined list of words which is loaded into the hardware based search engine. These words are automatically searched for during the next Capture session. At the end of the session, you can print one of several reports that indicate the number of occurrences, and absolute location on the drive of all matches found.

Searching for Keywords

Searching During Capture



1. From the Main Screen of the Dossier, tap the Settings icon.
2. Choose either Mirror or DD Image Capture mode.
3. Set all of the optional cloning settings as desired (verify, speed, etc.)
4. Tap the 'Word List' icon.
5. The unit will read the list of available keyword lists from the Compact Flash, and display it on the screen.
6. Choose the desired list, and press the OK icon.

NOTE: As of this writing, matches during capture are automatically logged in the capture report. Other settings will be accessible in later versions of the software under the **On Match** icon. Please contact Logicube for availability.

7. From now on, the words in this list will be searched for as a by-product of any of the Capture modes.
8. At the end of a session, the Final Capture report will also list any keywords found. You can then print one or both Keyword Search reports:



- **Print Search Detail:** This report lists every keyword found and the sector where it resides.



- **Print Search Text:** This report lists every keyword and the surrounding line of text.

NOTE: The DD Image Capture Report will not automatically list keywords. We suggest running the Search Detail report after the Capture Session to list any keywords found.

NOTE: Please refer to **Chapter 3. Drive Capture Modes and Settings** for more printing options.

Searching with Keyword Search Mode



In addition to searching for Keywords during a capture, the Dossier can also perform a separate Keyword Search session.

NOTE: If a Flash Media Card is chosen for a Keyword Search then the speed will drop to PIO-AUTO.

Procedure

1. From the Main Screen, tap the Settings icon to enter the Settings menu.
2. Tap the Keyword Search icon.
3. Tap the "Drives" icon. Choose one of the following drives: S1, S2, D1, D2, D1 & D2 or Flash.
4. Tap the "Speed" icon to set the desired UDMA or PIO speed.
5. Tap the 'Word List' icon.
6. The unit will read the list of available keyword lists from the Compact Flash, and display it on the screen.
7. Choose the desired list, and press the OK button.



8. Press the Start/Stop button twice to begin scanning.
9. Enter a Log file name and press SET.
10. At the end of a session, the Final Capture report will also list any keywords found. You can then print one or both Keyword Search reports:



- **Print Search Detail:** This report lists every keyword found and the sector where it resides.



- **Print Search Text:** This report lists every keyword and the surrounding line of text.

NOTE: The DD Image Capture Report will not automatically list keywords. We suggest running the Search Detail report after the Capture Session to list any keywords found.

NOTE: Please refer to **Chapter 3. Drive Capture Modes and Settings** for more printing options.

Keyword Lists

All keyword lists are stored on the Compact Flash in a file called keyword1.lst. The file is a simple text file which can be edited by any plain text editor, such as Notepad. The file can also contain hexadecimal values.

A sample file might look like this:

[Terrorism]

ABU NIDAL=case:yes,unicode:no,signature:no
 ABU SAYYAF=case:yes,unicode:no,signature:no
 AL-QAIDA=case:yes,unicode:no,signature:no
 BLACK SEPTEMBER=case:yes,unicode:no,signature:no
 DEMORALIZE=case:yes,unicode:no,signature:no
 HAMAS=case:yes,unicode:no,signature:no
 HIZBALLAH=case:yes,unicode:no,signature:no

[Computer crimes]

2600 =case:yes,unicode:no,signature:no
 BACK ORIFICE=case:yes,unicode:no,signature:no
 CRACK=case:yes,unicode:no,signature:no

DEFCON=case:yes,unicode:no,signature:no
ENCRYPTION=case:yes,unicode:no,signature:no
FLAME=case:yes,unicode:no,signature:no
HACK =case:yes,unicode:no,signature:no
IP SPOOFING=case:yes,unicode:no,signature:no

In the above example, two lists ([Terrorism] and [computer Crimes]), are listed. You can select only one for each search session. Many more lists with many more words can be defined.

Three options are available for each word:

1. **Case:** - yes/no. If Yes, the word is searched exactly as typed. No will search for all lower-case, all upper case, and First letter upper-case.
2. **Unicode:** yes/no. If No, the plain ASCII of the word will be searched for. Yes, the Unicode encoding of word is searched for.

NOTE: The Unicode search utilizes the “little endian” code that is utilized by Microsoft operating systems. Other systems, like Linux, UNIX, Mac, etc. utilize the “big endian” code. A future version of the Dossier software will also support big endian Unicode.

3. **Signature:** the word is only searched at the beginning of sector. This is useful to find all files of a certain type, e.g. all graphic files.

The unit allows some editing of the keyword lists. Please refer to the **Modify Lists** section below for more details.

NOTE: As of this writing, only the English alphabet is supported. Future software updates will include support for different languages. Please contact Logicube for further details.

Modify List Settings

Keyword Lists can also be created, modified and deleted from the Dossier itself. The following settings are accessed from the Optional Preference Settings under Keyword Search or by using the More button to access the Optional Preferences under Capture and DD Capture.

Modify Lists



Follow this procedure to directly access the Modify Lists menu:

1. From the Main Screen, press the Settings icon.

2. Press the Search icon.
3. Press the Modify List icon.
4. Three sub-menu functions appear:



- **Add New List:** This setting allows you to add a new Keyword Search List to the Compact Flash Card. When selected, you will see the words Enter new list name at the top of the screen. Enter the new list name and press Set and a screen will prompt you to add a Keyword to the list you just created. At this point you have an opportunity to assign whether or not Case Sensitivity, Unicode and Signature are to be factored into the search criteria. Enter YES or No for each of these setting and press the Set icon when finished. You can continue to add more keywords to the list at this time by pressing the Add icon. Once all of the Keywords have been added you must press the Save icon to add the new list.

Pressing Abort at any time will take you back to the Modify List Menu



- **Edit List:** This setting allows Keywords in existing lists to be modified or removed. It also allows new Keywords to be added. When selected, the Dossier will ask which list needs to be modified. Use the arrow icons on the screen to scroll through the list of file names. Once the list you wish to edit is located press the OK icon. The contents of the list and several selectable icons will display along the bottom of the screen. The icon choices within Edit List are:
 1. Add which allows you to add a new Keyword to the List.
 2. Edit which allows you to modify the Keywords Name, Case Sensitivity, Unicode and Signature search criteria.
 3. Delete which removes the Keyword from the list.
 4. Save which is a necessary step for the changes to be written to the CF card.
 5. Abort which will take you back to the Modify List Menu.



- **Remove List:** This setting removes a chosen list from the Compact Flash Card. When selected, the tool asks which list needs to be removed. Use the arrow icons on the screen to scroll through the list of file names. Once the Search List is located press the OK icon.

WARNING: There is no “are you sure” screen either when a list is chosen or before tapping OK for removal.

Pressing Abort at any time will take you back to the Modify List Menu.

Press the Back icon in the Modify List Menu will take you back to the Main Screen.

8. Optional Peripherals

Introduction

Logicube has many different adapters and other peripherals that allow you to tackle almost any drive capturing job. This chapter focuses on six particular devices – the Massive Portable Forensic Storage (MPFS™), the NETConnect™, the Clone Card Pro™, the Portable Battery Pack, the SCSI Adapter, and the SAS Adapter.

Massive Portable Forensic Storage (MPFS™)



Forensic investigators who need to capture large amounts of evidence data or need to transport sensitive data from the field to the lab will appreciate the convenience of the MPFS.

The MPFS provides up to 8 TB of forensic data storage and connects seamlessly to the Forensic Dossier data capture solution. Users can capture forensic data from suspect hard drives via the Dossier directly into evidence drives stored safely and securely within the MPFS. The MPFS eliminates the need to handle bulky sets of hard drives and reduces the risk of damaging sensitive hard drives during transport or compromising chain of custody.

A small footprint and convenient recessed “grip” areas on each side of the chassis make the MPFS easy to transport. The “always-on” cholesteric display allows users to identify contents at a glance making it convenient for archiving evidence data for future analysis.

Features

- Provides up to 8 TB of write-protected data storage in a 4 drive tray configuration
- Supports 3.5" SATA drives, (each drive with a maximum capacity 2 TB), arranged in a 2 or 4 drive configuration
- The MPFS works seamlessly with the Forensic Dossier. Simply connect the Dossier "head" to the MPFS base to immediately capture suspect drive data directly to the MPFS (will support both DD image and E01 file format capture modes, will not support Native capture mode)
- Stores multiple evidence capture sessions to hard disk drives in a JBOD configuration
- The MPFS features a compact footprint which makes it easy to transport from field to lab environments
- The Cholesteric "always on" battery-powered display requires no power and allows you to identify contents by file/case names at a glance
- Available without hard disk drives or in 4 "drive-populated" versions; 1 TB, 4 TB, 6 TB and 8 TB
- Multiple cooling fans to protect your data
- The MPFS allows direct connection to a PC via FireWire 400, USB 2.0 or eSATA. Write-protected ports allow you to preview or transfer data from the MPFS to a PC. **(Note: When using the FireWire and USB ports for data transfer to a PC, MPFS will support a maximum capacity of 2 TB. eSATA port must be used for capacities greater than 2 TB. A 64-bit Operating System must be used for capacities greater than 2 TB)**
- The MPFS features a ruggedized chassis that provides superior protection to hard drives stored in MPFS
- Compatible with the NETConnect network module

System description

The MPFS includes the following:

- USB and eSATA cables

- Power supply
- Users' Guide on CD-ROM
- Magnetic screwdriver
- "0" drive configuration ships with drive mounting brackets and hardware to install hard disk drives
- Other configurations ship with hard drives pre-installed by Logicube

Connecting the Forensic Dossier to the MPFS

The Dossier head attaches to the MPFS. Follow these steps to attach the two parts together:

WARNING: The Dossier head is not hot swappable with the Dossier tray and the MPFS. Power must be unplugged from the Dossier head before attaching it to the MPFS or the Dossier tray.

1. If necessary, disconnect the Dossier head from the Dossier tray by turning the tabs on each corner of the unit as shown in Figure 8:



Figure 8, Opening corner latches.

2. Lift the top (or "head") off the bottom of the unit as show in Fig. 9:

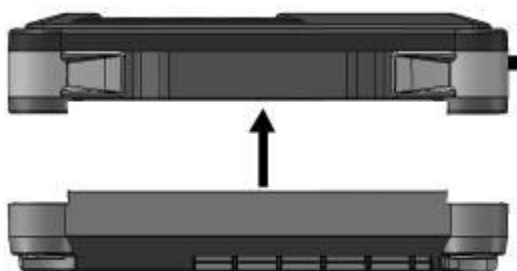


Figure 9, Lifting head off unit.

3. The bottom of the Dossier head may have four foam pads. To connect the Dossier head to the MPFS these foam pads must be removed.
4. Attach the Dossier head to the top of the MPFS and turn the corner latches to lock the Dossier head in place.
5. Once the Dossier head is attached to the MPFS, the power and connector ports on the MPFS™ are not accessible. Attach the power adapter to the Dossier head to turn on the unit.

Usage Notes: For more information on how to use the MPFS with the Dossier Tray, consult the MPFS manual.

The Logicube NETConnect is designed to work in conjunction with the Logicube Forensic Dossier and MPFS. The NETConnect provides the convenience of allowing multiple investigators to access a single set of case files, streamlining the analysis process by allowing broad access either locally or remotely to the evidence data post capture.

Features

- Works seamlessly with the Forensic Dossier and MPFS
- Uses CIFS, NFS or FTP file access protocols
- 10/100/1000 Gigabit Ethernet interface
- Supports Windows, MAC, Linux operating systems
- Data transfer rate approaching 7GB/min
- Network protocols supported include ARP, IP, UDP, TCP, HTTP, ICMP, BOOTP/DHCP, DNS, MDNS, Telnet
- NETConnect can be configured as a “client” for a network file system or as an actual network file system server or NAS
- Allows you to “push” or transfer evidence data to pre-defined network destinations, verify network transfer, format and wipe drives
- Administrative functions allow users to establish user names, passwords, manage access control, maintain credentials, set destination IP addresses and domain names
- Convenient “Macro” feature allows users to easily initiate preconfigured commands from the control panel of NETConnect

Connecting NETConnect to the Forensic Dossier tray

The Logicube NETConnect can be attached to the Logicube Forensic Dossier tray or the Logicube MPFS allowing easy access to the hard drives used either with the Forensic Dossier tray or the MPFS.

Please note that all drives attached in the Logicube Forensic Dossier tray, when attached to the NETConnect, must be set to 1.5

Gigabits per second. Typically, instructions on how to set hard disk drives to 1.5 Gb/s can be found on the label of the hard disk drive. If instructions are not found on the label, please check the hard disk drive manufacturer's website for more support.

To connect the NETConnect to the Forensic Dossier tray, follow the instructions below:

1. Ensure that power and all cables attached to the Dossier have been disconnected.
2. Turn the tabs on each corner of the unit as shown in Fig. 1 below:



Figure 1, Opening corner latches.

3. Lift the top (or "head") off the bottom of the unit as shown in Fig. 2 and set the Dossier head aside.

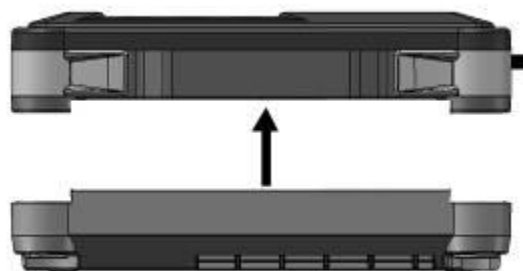


Figure 2, Lifting head off unit.

4. Set the NETConnect on top of the Dossier tray and make sure the NetConnect underside connector aligns with the Dossier tray's connector as shown in Fig. 3 below:

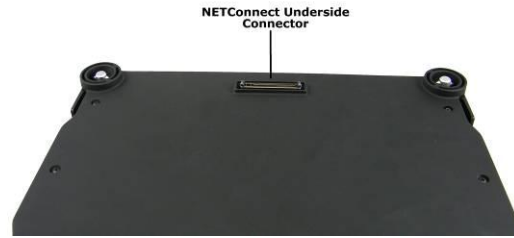


Figure 3. NETConnect Underside Connector

5. Close the front and back side latches to lock the NETConnect in place.

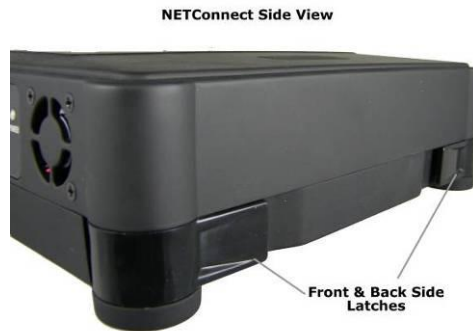


Figure 4. Front & back side latches

Usage Notes: For more information on how to use the NETConnect with the Dossier Tray, consult the NETConnect manual.

Logicube Clone Card Pro™

The optional CloneCard Pro is an intelligent PCMCIA adapter designed to provide fast cloning to and from laptop PC's. When used properly, it will support up to 115 MB/min transfer speed.

The CloneCard Pro is a real time-saver when a laptop drive needs to be captured, and it is undesirable to remove the internal hard drive from the PC. It is designed to work in both PCMCIA (16-bit) and CARDBUS (32-bit) systems.

In general, the user would boot the laptop from the supplied CD-ROM and run a client program. This client program detects the PCMCIA chip-set inside the laptop and will enable communication to the CloneCard Pro. Now the Dossier can be connected to the external cable of the card, and operation commences as if the Dossier is connected directly to the suspect drive. All Dossier modes and options are operational as though an actual drive is

connected, with the exception of the speed of transfer.

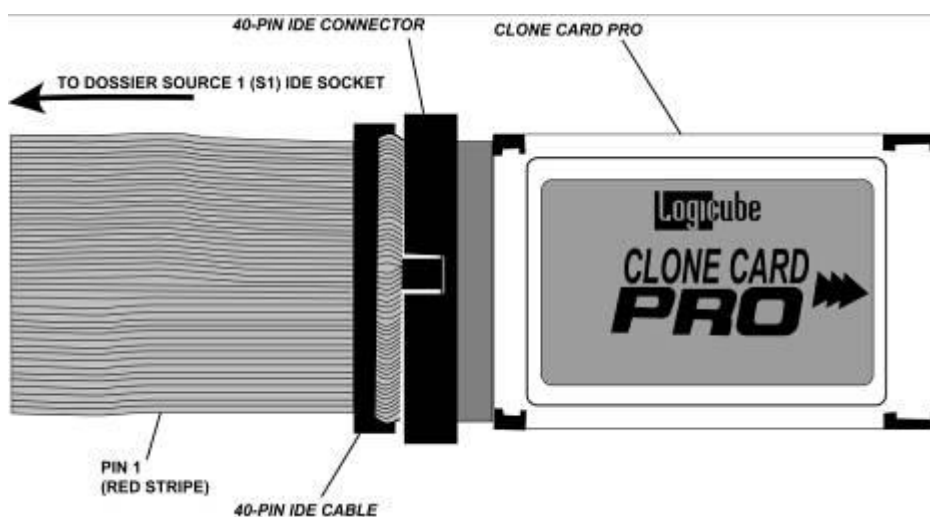


Figure 12, Clone Card Pro

Before Capturing

Logicube provides a bootable CD-ROM which runs off the FREEDOS operating system. Follow the loading directions that come with your Clone Card Pro.

Using the Logicube CloneCard Pro to Capture a Drive

Cloning with the CloneCard takes just a few steps.

1. Insert the CloneCard Pro into one of the PCMCIA slots on the laptop you are about to clone (make sure to remove all other PCMCIA cards).
2. Insert the CD-ROM into the laptop CD drive.
3. Turn laptop on. Ensure that the laptop is set to boot from a CD-ROM. This is done through the

setup screens that can be accessed by pressing F2 or <DEL> key during initial boot (consult your laptop manual regarding how to set the boot order).

4. The CD-ROM is configured to run the client application (CCclient.exe or pcmcia.exe) automatically.
5. Connect the S1 position of the Dossier to the flat cable provided with the CloneCard Pro.

Do not use one of the Dossier's included PATA drive cables. They are incompatible with the CloneCard Pro!

6. Make all the necessary settings on your Dossier.
7. Set the Speed setting to PIO-Slow. No settings are available on the client program.
8. Press the **START/STOP** button and wait for the process to complete.

Improving Speed of Transfer

Several settings in the CMOS setup screens can potentially improve the speed of transfer.

1. **PCI latency timer** - Try to reduce the value of this number as much as possible.
2. **PCI write buffer** - Set to enable to improve writing speed to the local drive.
3. **PCI zero-wait states** - Enable to decrease PCI cycle time.
4. **PCI delay transaction** - Disable to decrease PCI cycle time.
5. **PCI dynamic bursting** - Set to yes.
6. **Enable 32-bit access to hard drive** - We test for that, and if available, we use it to improve transfer speed, so no action is required on behalf of the user.

NOTE: Some of these settings may not be present on your machine. Also, some of these settings may cause other peripherals to not function properly, so use with caution, and always change one setting at a time.

Logicube Portable Battery Pack

The optional rechargeable battery pack (Logicube P/N **F-BATTERY-EXTND**) is used to power the Forensic Dossier whenever connection to a standard AC outlet is either undesirable or not possible. This guide is intended to provide users with connectivity instructions unique to this rechargeable battery pack and the device it is designed to support.

Precautions

- Do not charge the battery pack in a gas tight container. Charge only in well ventilated areas
- Do not short the battery terminals or battery pack connector pins with metal objects
- Do not incinerate the battery
- Immediately flush with water for at least 15 minutes after physical contact with electrolyte (Acid)
- Always store the Portable Battery Pack in a cool dry ventilated area away from combustibles
- Use caution when lifting or carrying the battery to prevent injury

What's Included

- QTY 1 Battery Pack **P/N F-BATTERY_EXTND**
- QTY 1 Power Out Cable for connection between the Portable Battery Pack and the Forensic Dossier or to daisy chain additional battery packs together

Charging the Battery – Dos & Don'ts

1. A protection circuit prevents the battery from being over charged if the pack is left connected to the charger.
2. The *Power Out & Charge* female mating connectors on the battery each have three and four pins respectively and are keyed to simplify cable connection. Special care should be taken when inserting cables into the battery pack in order to prevent damage to the connectors.

Connecting Battery to Charger

The Forensic Dossier power supply can be used to charge the portable battery pack.

1. Plug the AC power cord that came with the Forensic Dossier between the AC input of the Dossier power supply and a grounded AC outlet.
2. Locate the four pin cable opposite the AC input of the Dossier power supply and plug the cable into the battery pack connector labeled CHARGE.
3. At this point an Amber colored LED will illuminate next to the word CHARGING irrespective of the position of the on/off switch. This amber LED indicates the battery is charging. A row of five LED's grouped together indicate the batteries current charge status and become visible during charging or anytime the power switch is in the ON position. See Figure 16 for details.
4. In order to achieve full charge capability the battery pack needs to be charged for approximately 9 hours.

Figure 16



Connecting Battery & Device

- Use the supplied POWER OUT cable to connect the Portable Battery Pack POWER OUT connector to the Forensic Dossier power input connector labeled **12V**
- Use the ON/OFF switch on the Battery Pack to power up the Forensic Dossier

Connecting Multiple Batteries

- Users can increase usable capture time by purchasing additional Battery Packs from Logicube Inc. and daisy chaining batteries together
- At any time during capture mode or whenever the solid red LED status light is on, users can physically attach the supplied "POWER OUT" cable from an additional battery (Fully Charged) to the "CHARGE" connector of the battery pack currently powering the Forensic Dossier

Additional Considerations

- A fully charged battery pack has been shown to provide power to the Forensic Dossier hard drive capture device for periods of up to 3hrs of use
- It is safe to charge the Portable Battery Pack at any time during a Forensic capture

Waste Disposal Method

- Federal and State laws prohibit the improper disposal of all lead acid batteries. The battery pack end users (owners) are responsible for their batteries from the date of purchase through their ultimate disposal. The only legally acceptable method of disposal of lead acid batteries is to recycle them at a Resource Conservation and Recovery Act (RCRA) approved secondary lead smelter

NOTES: When storing the battery pack, turn the switch to the OFF position and charge the battery at least once every month to prevent possible damage to the battery.

A flashing RED status LED indicates the battery can supply power for approximately 20 minutes of continued operation. The charger should be plugged into the battery immediately if you are in the middle of a drive capture.

Only the FULLY CHARGED LED will remain illuminated after the battery has been in the fully charged state for approximately one hour.

Logicube SCSI Adapter

The Logicube SCSI adapter is designed to attach directly to specific Logicube HDD duplication devices. Functionally the adapter acts like a pass through device and allows for external connection and capture of SCSI drive data through the IDE port of the Logicube Forensic Dossier. Optionally, USB and USB Thumb/Flash drives can also be captured through the adapter.

The SCSI adapter is designed to capture from SCSI to SATA/IDE not from SCSI to SCSI type drives.

NOTE: The Optional SCSI Adapter is compatible with the Forensic Dossier but does not support Wipe or capture from RAID pairs.



Figure 17 SCSI Adapter

What's Included

- Qty. (1) F-ADP-SCSI Adapter
- Qty. (1) CBL-031A SCSI Ribbon Cable
- Qty. (1) CBL-002B Power Cable

What's Needed

- Qty. (1) CBL-037B IDE Ribbon Cable
- Qty. (1) CBL-002B Power Cable

NOTE: These cables ship with the Forensic Dossier

Installation Setup

1. Disconnect the power supply cord from the Logicube Forensic Dossier.
2. Locate the IDE ribbon cable P/N CBL-037B and plug the end labeled HDD SIDE into the SCSI adapter port marked IDE CONNECTOR IN.
3. Connect the other side of the ribbon cable labeled DUPLICATOR SIDE to an external IDE port on the Dossier.
4. Locate the cable labeled CBL-002B and connect the end with the large white plug to the mating receptacle next to the IDE ribbon cable on the SCSI adapter.
5. Connect the other side of the CBL-002B to the external power port of the Dossier. Use the power port closest to the ribbon cable.
6. To capture a SCSI drive connect one side of cable CBL-031A to the SCSI HDD and plug the other side into the connector on the SCSI adapter located below the label SCSI CONNECTOR.
7. Connect one end of CBL-002B (power cable #2) between the adapter connector labeled SCSI POWER and the mating receptacle on the SCSI HDD.

How to use the SCSI Adapter

Duplicating using Forensic Dossier

1. Install one or two destination hard drive(s) inside the Logicube Forensic Dossier.

NOTES: For forensic captures the destination drive(s) should be at least as large as the drive(s) to be captured. The exception is if you are using the Dossier's Spanning mode which allows you to capture across two destination drives.

When two SAS adapters are used to forensically capture two SAS suspect drives care should be taken to prevent the drives controller cards from shorting out on any exposed metal.

Capture from HPA and DCO areas is not supported.

2. Reinsert the power supply cord to turn on the Logicube Dossier. The LED located on top of the SCSI adapter near the RESET button will illuminate solid green indicating that the adapter is receiving power correctly.
3. At this point you can perform a standard drive info check to verify that the Logicube Forensic Dossier recognizes the drive connected through the SCSI adapter.
4. Adjust the Forensic Dossier capture settings as desired.
5. Start the capture process according to the instructions outlined in the Dossier User's Manual under Capture Modes and Settings.

NOTE: Native, DD and E01 type forensic captures are supported using Dossier in conjunction with the SCSI adapter. (E01 is supported from SW release 1.17 and firmware 8.15 forward).

Optional USB cloning with the SCSI Adapter

In order to use the USB port located on the Logicube SCSI Adapter, the USB cloning option must have been purchased and the feature enabled on the cloning device to which the adapter is connected. To verify if the USB cloning feature has been enabled, turn on the Logicube cloning device and press the About icon on the main menu. If *SCSI Adapter USB Option* is visible under Options installed; you can tap the BACK icon and continue to the next step. If *SCSI Adapter USB Option* is not in the list the feature has not been enabled. To verify if the option has been purchased contact Logicube Technical Support and provide the S/N of the cloning device listed at the top of the About screen. Once you have obtained an activation code follow the activation instructions listed below to enable the USB cloning feature.

Press Misc., More, Install Options, [Enter the code] and press the SET button. Once complete the About screen will read: *Options installed: SCSI Adapter USB Option* along with any other options that may be installed.

- To clone or capture a USB powered HDD connect a USB cable between the USB Drive and the SCSI adapter connector labeled USB PORT and proceed to step 1 the Duplicate Using section.

- To clone or capture a USB thumb drive connect the USB thumb drive directly into the SCSI connector labeled USB PORT and proceed to step 1 of the Duplicate Using section.

NOTE: A second LED located on top of the SCSI adapter will flash green during adapter control and whenever data transfer occurs.

The RESET button on the side of the SCSI adapter located next to the USB PORT is not active at this time and is reserved for future enhancements.

USB functionality via the SCSI adapter is tied to the S/N of the cloning device that receives the activation code. Once the USB option is activated, the USB cloning feature can only be used in conjunction with that specific cloning device.

SCSI/USB enabled Dossier may be able to clone flash media cards by using a USB multi card reader in conjunction with the SCSI adapter. Note that this functionality has not been fully verified and is not guaranteed.

Logicube SAS Adapter

The Logicube SAS adapter is designed to attach directly to the Logicube Forensic Dossier. Functionally the adapter acts like a pass through device and allows for external connection and capture of SAS drive data through the IDE port of Dossier. Optionally, USB and USB Thumb/Flash drives can also be captured through the adapter.

The SAS adapter is designed to capture from SAS to SATA/IDE not from SAS to SAS type drives with Dossier.

NOTE: The Optional SAS Adapter is compatible with the Forensic Dossier but does not support Wipe or capture from RAID pairs.



Figure 18 SAS Adapter

What's Included

- Qty. (1) F-ADP-SAS Adapter
- Qty. (2) CBL-SAS-001-A SAS Data/Power Cable

What's Needed

- Qty. (1) CBL-037B IDE Ribbon Cable
- Qty. (1) CBL-002B Power Cable

NOTE: These cables ship with the Forensic Dossier

Installation Setup

1. Disconnect the power supply cord from the Logicube Forensic Dossier.
2. Locate the IDE ribbon cable P/N CBL-037B and plug the end labeled HDD SIDE into the SAS adapter port marked IDE CONNECTOR IN.
3. Connect the other side of the ribbon cable labeled DUPLICATOR SIDE to an external IDE port on the Dossier.
4. Locate the cable labeled CBL-002B and connect the end with the large white plug to the mating receptacle next to the IDE ribbon cable on the SAS adapter.
5. Connect the other side of the CBL-002B to the external power port of Dossier. Use the power port closest to the ribbon cable.

6. To clone a SAS drive connect one side of cable CBL-SAS-001-A to the SAS HDD and plug the other side (which splits and forms the shape of a 'Y') into the SAS data and power ports located on the SAS adapter above the label MASTER and proceed to step 1.

How to use the SAS Adapter

Duplicating using Forensic Dossier

1. Install a destination hard drive inside the Logicube Forensic Dossier.

NOTE: For forensic captures the destination drive should be at least as large as the drive to be captured.

2. Reinsert the power supply cord to turn Dossier on. The LED located on top of the SAS adapter near the RESET button will illuminate solid green indicating that the adapter is receiving power correctly.
3. At this point you can perform a standard drive info check to verify that the Forensic Dossier recognizes the drive connected through the SAS adapter.
4. Adjust the Forensic Dossier capture settings as desired. When ready, start the capture process according to the instructions outlined in the Dossier User's Manual under Capture Modes and Settings.

NOTE: Native, DD and E01 type forensic captures are supported using Dossier in conjunction with the SAS adapter. (E01 is supported from SW release 1.17 and firmware 8.15 forward).

Optional USB cloning with the SAS Adapter

In order to use the USB port located on the Logicube SAS Adapter, the USB cloning option must have been purchased and the feature enabled on the cloning device to which the adapter is connected. To verify the USB cloning feature has been enabled, turn on the Logicube cloning device and press the About icon on the main menu. If *SAS Adapter USB Option* is visible under Options installed; you can tap the BACK icon and continue to the next step. If *SAS Adapter USB Option* is not

in the list the feature has not been enabled. To verify if the option has been purchased contact Logicube Technical Support and provide the S/N of the cloning device listed at the top of the About screen. Once you have obtained an activation code follow the activation instructions listed below to enable the USB cloning feature.

Press Misc., More, Install Options, [Enter the code] and press the SET button. Once complete the About screen will read: *Options installed: SAS Adapter USB Option* along with any other options that may be installed.

- To clone a USB powered HDD connect a USB cable between the USB Drive and the SAS adapter connector labeled USB PORT and proceed to step 1 of the appropriate Duplicate Using section for your device.
- To clone a USB thumb drive connect the USB thumb drive directly into the SAS connector labeled USB PORT and proceed to step 1 of the appropriate Duplicate Using section for your device.

NOTES: A second LED located on top of the SAS adapter will flash green during adapter control and whenever data transfer occurs.

The RESET button on the side of the SAS adapter located next to the USB PORT is not active at this time and is reserved for future enhancements.

USB functionality via the SAS adapter is tied to the S/N of the cloning device that receives the activation code. Once the USB option is activated, the USB cloning feature can only be used in conjunction with that specific cloning device.

A SAS/USB enabled Dossier and may be able to clone flash media cards by using a USB multi card reader in conjunction with the SAS adapter. Note that this functionality has not been fully verified and is not guaranteed.

9. Internal Flash Memory

Introduction

The Logicube Dossier comes with an internal Compact Flash (CF) Card that is in a covered slot underneath the lid of the unit. This drive is used mostly for loading software and firmware on the Dossier, storing Keyword Search lists and storing session reports.

NOTE: Please check our website periodically at www.logicube.com, any new CF functions will be posted there.

To load new software from the CF Drive, please refer to **Chapter 10. Software and Firmware Loading Instructions**

Connecting the CF Drive to Windows via USB or FireWire

This procedure is necessary to load new software files to the System CF card. It is also necessary to pull session reports off the Dossier and add new Keyword lists created on the PC.

Connecting Through USB or FireWire Mode

1. Make sure your PC is running Win98 or above.
2. Connect the USB or FireWire cable (provided) to a PC USB or FireWire port on one end. Do not attach the other end to the Dossier yet.
3. From the Main Screen of the Dossier, tap the Settings icon or press the Set button.
4. Press the USB / FireWire icon.
5. Tap the USB or FireWire icon, 2 settings will appear:



- **Drives:** Choose System CF (Dossier's internal flash memory).
6. The Dossier will power up the chosen drive. A prompt will appear that reads "USB Link Up" or "FireWire Link Up".
 7. Press Start/Stop twice.

8. Attach the USB or FireWire cable to the Dossier. You should now see some activity on your PC screen, which depends on the operating system.
9. If running ME/2000/XP/Vista/7 your drive will automatically be mounted and drive letters assigned to all recognizable partitions.
10. If running 98/98SE you will be prompted to install drivers. At the "have disk..." prompt please point the PC to the drivers floppy (provided), and the installation should complete smoothly.
11. The System CF is now visible on Windows as an external drive. The System CF drive is not write-protected, so files can be modified on the card itself.

Removing USB devices

Before physically disconnecting the USB cable and/or shutting down power to the Logicube Forensic Dossier, the unit has to be properly "unmounted" from Windows. To do that:

1. Locate the USB icon in the system tray (typically at the bottom right of screen).
2. Click the icon once.
3. Wait for Windows to bring up a message that it is safe to remove the device. (Different versions of windows will behave slightly differently).

Installation and Removal of Internal CF Drive

In rare occasions, it may become necessary to replace the CF drive that is located inside the lid of the Dossier.

NOTE: Only follow this procedure if you are comfortable with opening computers and replacing components. If not, and you are experiencing memory card problems, please contact Logicube technical support.

Internal Flash Memory Removal and Installation

1. Unplug the Dossier from the power supply.
2. Remove the head (top half) of the Dossier like you are going to attach a Destination drive.
3. Turn the head over so that the bottom is facing up.

4. Use a Phillips head screwdriver to remove the four screws holding the small access panel to the underside of the head.
5. Remove the access panel to expose the CF Card.
6. Carefully remove the CF card by sliding it off the CF card holder.
7. Replace the CF card with a new card that is formatted using the FAT (not FAT32 or NTFS) filesystem and contains the following files:
 - fpga.rpd
 - fpgaE01.rpd
 - fpgaE01D.rpd
 - fpgav1.rpd
 - ngf.bin
 - NGF.INI
 - NGFBIOS.BIN
 - ngfv1.bin
 - ngfv2.bin
 - NTFSFRM.FTM
8. Insert the replacement CF card back to the CF card slot.
9. Replace the access panel and the four screws.

10. Software and Firmware Loading Instructions

Introduction

New and improved software will appear from time to time on our web site at www.logicube.com. It is possible to update both the operating software and the firmware in the field by a user.

NOTE: Logicube provides a CD-ROM that contains a backup copy of the Dossier software. This software is already loaded on your unit.

Software version 2.0.0RC01-105 and is not compatible with the MPFS. In order for you to use the Forensic Dossier with MPFS you must revert to software version 1.21RC50 and firmware version 9.0. Instructions on how to do this can be found below.

NOTE: See the “MPFS (Maassive Portable Forensic Storage) Notes” below.

Loading New Software and Firmware

The new software and firmware have to be placed on the root directory of the System CF card.

1. Disconnect the AC Adapter from the Dossier, and hold down the Start/Stop button while re-connecting the AC Adapter back on.
2. A hidden menu will appear with the following choices:

Continue – This boots the unit to the Main screen.

Upgrade FPGA Firmware – replaces the current firmware with the newest firmware file (no longer used).

Engage System CF card – engages the CF card and makes it accessible through the USB connection.

3. Use the Back button to scroll to “Engage System CF card” and press the Set button to confirm your selection.
4. The Dossier will apply power to the System CF card. Attach a mini USB cable

- (included) to a Windows based PC and to the Dossier.
5. Windows will detect the System CF card and automatically assign a drive letter to the System CF card.
 6. Extract the contents of the downloaded zip file to the root of the System CF card and overwrite any existing file(s) on the System CF card.
 7. Press the BACK button to go back to the hidden menu.
 8. Disconnect the AC adapter from the Dossier. Wait at least 10 seconds then re-connect the AC adapter to apply power to the Dossier.
 9. The Dossier will load the new BIOS, Software, and Firmware during the boot process.
 10. Check the version and date of the new software and firmware by tapping the "About" icon at the Main Screen.

MPFS (Massive Portable Forensic Storage) Notes:

If you upgraded to this software release and want to use your Dossier with the MPFS, simply follow these instructions:

- A. Disconnect the AC Adapter from the Dossier, and hold down the Start/Stop button while re-connecting the AC Adapter back on.
- B. A hidden menu will appear with the following choices:

Continue – This bypasses the upgrade and boots the unit into the main screen.

Upgrade FPGA Firmware – Replaces the current firmware with the newest firmware file (no longer used).

Engage System CF card – Engages the CF card and makes it accessible through the USB connection.

- C. Use the Back button to scroll to "Engage System CF card" and press the Set button to confirm your selection.
- D. The Dossier will apply power to the System CF card. Attach a mini USB cable (included) to a Windows based PC and to the Dossier.

- E. Windows will detect the System CF card and automatically assign a drive letter to the System CF card.
- F. Delete the file ngfv2.bin.
- G. Press the BACK button to go back to the hidden menu.
- H. Disconnect the AC adapter from the Dossier. Wait at least 10 seconds, then re-connect the AC adapter to apply power to the Dossier.
- I. The Dossier will revert back to software version 1.21RC50 and firmware version 9.0. Check the version and date of the software and firmware by tapping the "About" icon at the Main screen.

NOTE: If you want to use the Dossier with the Dossier tray and any new feature featured in software releases 2.0.0RC01-105 and up you must follow steps A through E above then extract the ngfv2.bin from the downloaded zip file to the root of the CF card, then follow steps G and H. The newer version of the software will load during the boot process. Check the version and date of the software and firmware by tapping the "About" icon at the Main screen.

11. Reference

Further Notes on Modes Available for the Dossier

Capture – Native or DD image

This process captures all data from the source drive to the destination drive. See the “**Anatomy of a Drive Capture**” section below for more information.

Drive Defect Scan

The Drive Defect Scan operation performs a surface scan of the drive media using the drive controller to verify the media. This is done without transferring any data from the drive and results in extremely fast operation at the maximum media speed of the drive. This is typically faster than the maximum sustained transfer speed of the drive. The media is scanned in blocks of 256 sectors. If a block fails to verify, it is retried once at the block level. If it fails again, each of the 256 sectors is scanned individually. Each sector is scanned up to ten times. If a sector fails immediately, it is classified as bad. If the sector fails to verify after a good read any time up to the tenth read it is classified as weak. If the sector is verified good for ten reads it is classified as good. If, after the individual sectors are all scanned and there are no bad sectors found, the block is classified as a weak Spot.

Options

Drive – Choices are S1, S2, D1, D2 or Flash

Speed – The choices are Fast or Slow

Wipe Destination

The Wipe Destination function is the process that erases or wipes all existing information from the surface of destination disk drive.

Options

These are the user configurable options for the Dossier erase process.

Speed – The speed setting provides the option to set the speed at which an operation will be performed.

The choices are UDMA-6 to UDMA-0, PIO-AUTO, PIO-MED and PIO-SLOW.

Signature – A unique digital signature is written to the destination drive on the first sector of each logical cylinder boundary across the entire drive.

Choose Yes or No

Erase process with Security Erase.

The software sends an ATA command to the drive to instructing it to erase itself as per its manufacturer's specification.

Erase process using non Security Erase drives

The software will do a CPU-erase. This is a process where the Dossier's CPU writes a pattern of 0's to the drive.

Additional Commands

Verify

The Verify option adds an increased level of confidence in the capture process. The choices are: HASH, HASH + V and None.

HASH

This mode uses special hardware to compute SHA-256 and MD5 Hash values at an extremely fast and accurate rate.

NOTE: If the Destination drive has bad or weak sectors, this mode may not guarantee the accuracy of the Hash values. If the destination drive's health is unknown, use the "+V" setting.

HASH + V

This mode uses special hardware to compute SHA-256 and MD5 Hash values at an extremely fast and accurate rate. It also performs a read-back and comparison of each block of data as it is captured. It is highly recommended that this mode be selected to ensure the accuracy of the Hash values.

None

(Default setting) This method performs no special verification and is used only for non-forensic cloning purposes.

On Error

The On Error option controls what actions are taken when the software runs into problem areas on the source drive. The choices are:

ABORT – The Abort option causes the software to stop the copying process and display an error message when an unreadable area is encountered on the source drive.

SKIP – The Skip option causes the software to ignore a bad sector and not copy it to the destination drive. All prior and subsequent sectors are copied while only the unreadable sector is skipped. This Sector is filled with zeros on the destination drive.

RETRY – The Retry option attempts to reread an offending sector. The user can set the number of retry attempts from zero to 1,000 attempts. The default setting is 50. The Dossier uses the following sequence for retry:

1. Reinitialize the source drive.
2. Dump the drive's cache buffer.
3. Reread the offending sector. If a good read occurs then the retry loop is aborted immediately and copying continues.

If the sector is still unreadable after the maximum number of retries, then it is skipped and the copying process continues with the following sectors. As with the skip option, if the sector is skipped, it is filled with zeros on the destination drive.

RECOVER – At least one reinitialize and retry is performed for all choices before recovery is attempted. This prevents recoverable errors from halting the completion of the copying process. For all modes, except ABORT, the hardcopy printout will provide a list of sector numbers that failed.

The Recover option makes up to 50 attempts to reread an offending sector using the following sequence:

1. Reinitialize the source drive.
2. Dump the drive's cache buffer.
3. Reread the offending sector. If a good read occurs then the retry loop is aborted immediately and copying continues.
4. If the read failed, the low level code transfers the drive's buffer contents anyway. The buffer is examined and information is collected for a majority vote algorithm.

5. If the sector is still unreadable after the maximum number of retries, the software will then attempt to reconstruct the sector by applying a majority vote algorithm to the data collected while performing the retries. The sector is then written to the destination drive and the copying process continues with the following sectors.

Printer

The printer option contains a submenu with various functions controlling the generation of hardcopy printouts of Capture, DD Imaging, Scan or Wipe Sessions.

AUTO PRINT – The print report option controls whether or not a hardcopy printout is automatically generated immediately following a Capture, Scan, or Wipe session. The choices are YES, or NO.

PRINT LAST SESSION – The Print Last Session option enables the user to get a hardcopy printout of the previous Capture, Scan or Wipe session even if the Print Report option above was not enabled. As long as power remains applied to the unit, the previous session's results are available.

PRINT SEARCH DETAIL – Prints a detailed report of all words matched during the last session, and their absolute location

PRINT SEARCH TEXT – Prints a snippet of text before and after the matched word, for every word matched during the last session

EJECT PAGE – The Eject Page option is a utility function that will send a page eject or form feed command to the printer. This may be necessary when using certain kinds of laser printers.

Anatomy of a Drive Capture

The drive capture process implemented in the Dossier is a specific and detailed process designed to ensure maximum integrity and certifiable performance. It consists of a number of checks and procedures that are detailed in the following section.

Power-up and Initialization

Power and reset are applied to both source and destination drives, then the software waits for up to 30 seconds for the source drive to become ready.

When the source drive is ready, the software identifies the drive configuration and initializes drive parameters.

The software then checks the destination drive for ready status and waits, if necessary. When the destination drive becomes ready, the software identifies the drive configuration and initializes drive parameters.

If the initialization of either drive fails, the software aborts the process with an error message.

The software verifies that the destination drive capacity is equal to or greater than the source drive. If the destination capacity is insufficient, then the user is informed and the software will abort the capture process.

Log file name entry

The unit initializes the CF Drive, and then asks the user to enter a case name. If you are capturing from two source drives to two destination drives the unit will ask for two separate case names. Case name(s) must be less than 195 characters or less and use DOS naming conventions.

Note: When using Spanning mode the maximum character length is 193. For Mirror/Wipe/Scan/HASH modes the maximum length is 8 characters.

The Log file name is used for the report that is created at the end of the capturing session and written to the System CF Drive (if you are capturing from two source drives to two destination drives two reports will be generated). The report can be opened and printed from any text editor in Windows (like Notepad).

Calibrate Transfer Speed

If the Speed option described previously is set to any UDMA speed, then the calibration procedure is performed as follows:

1. In the drive identification process, the maximum speed of each drive is identified and stored.
2. The UDMA calibration process, simply takes the lowest common denominator of all drives involved in the process.

If none of the involved drives are UDMA capable, OR, if the Speed option described previously is set to any of the PIO speeds, then the following PIO calibration procedure is performed:

1. The transfer speed is set to a conservative initial value.

2. A chunk of the source drive is copied to the destination drive.
3. If there are no errors, then the elapsed time is stored. If there is an error, then the software will set the transfer speed to a lower value and exit the routine.
4. The transfer speed is set to the next higher value and the process is repeated until the highest speed is reached that does not result in any errors.

Check Capture Integrity

This procedure tests the integrity of the data path including the following items.

- Drive interface
- Data cables
- Unit integrity
- Loose connectors.

The method used is as follows:

1. For drives that are running at PIO speeds: All bits of the data lines of the source drive are checked for toggling between one and zero while reading data from the drive. This is necessary because the data lines can be broken or unreliable and we can still communicate with and control the drive without transferring data.

NOTE: For this test, the unit checks an 8 MB portion of the drive that starts 50MB from the start of the drive. If the drive is wiped, or there is no data in that area, then the unit will pause with an error: **“Source drive data lines cannot be identified. Do you wish to continue?”** Choose <Yes> to continue with the Capture or choose <No> to abort. If the capture is continued, then the error message will not show up on the final capture report.

NOTE: This step does not apply to Flash Media Cards, even though they run at PIO-AUTO speeds.

2. A chunk of the source drive is then copied to the destination drive at the speed previously set in the calibration procedure.
3. Every byte of every sector copied is then compared on the source and destination drives.
4. If the data on both drives match, then the software will exit the Integrity check and continue the capture process. If the data does not match, the transfer speed is lowered to the next available

setting. The process is then repeated until the data is identical on each drive.

NOTE: If a match does not occur, the unit will fail with an error.

Verify Destination Drive is Erased

Verify Erasure

The destination drive is checked to be sure it has been erased before copying the data from the source to the destination drive. Verifying the existence of a unique digital signature that is written to the drive during the Wipe-clean or erase function performs this check. The signature is written periodically across the entire drive when the Dossier erases it. If the drive is verified as erased, then the Capture process will proceed without any user intervention. If the erase is not verified, the user is asked if the drive should be erased now. If the user says yes, then the drive is erased and the Capture process will proceed. If the user declines, then this is noted and will show on the printed report. The Capture process will proceed.

Wipe Destination

The next section only applies if Wipe Destination is chosen during a capture session:

Eraser Process

The software will write zero-filled sectors directly to the entire destination drive using programmed I/O.

If the words Security Erasing show in the UI during the wipe the drive is Security Erase enabled.

If the word Erasing shows in the UI during the wipe the drive is not Security Erase enabled.

Write a unique signature to the destination drive.

By default, the software writes a unique digital signature to the destination drive on the first sector of each logical cylinder boundary across the entire drive. This enables the Capture process to quickly verify that the destination drive has been erased prior to the Capture process. The unique signature is written to the last 12 bytes of the sector. The data pattern is

0xAAAA, 0x5555, followed by the character string "Logicube".

If needed, the user can disable the signature by selecting "NO" on the "Signature" menu located in the settings menu.

Capture Source Drive Data To Destination Drive

All Data on the source drive is copied sector-by-sector to the destination drive.

Check for Erasure of Unused Portion of Destination Drive

If the destination drive has not been previously verified as erased and the source drive has less capacity than the destination drive, then the software will ask the user whether or not to erase the unused remaining portion of the destination drive. If the user accepts, then the remainder of the destination drive will be erased and the Capture process will continue. If the user declines, then this is noted and will show on the printed report. The Capture process will proceed. This is to ensure that there is no leftover data from any previous usage on the extra portion of the drive. Note: In the DD imaging modes, erasure of remainder of drive is not an option.

Print Final Capture Report

If the Auto Print setting was set to YES prior to Capture, then the unit will prompt the user with a message: "Make sure that the printer is connected, powered up and online. Press <OK> to print". Press the Select button to initiate printing. A Final Capture Report will then be printed.

If the Printer setting was set to NO prior to capture, then a report can still be printed as long as the unit hasn't been powered down, rebooted or used to clone more drives. Just go to the Misc Menu, tap the Print Options icon, tap the "Additional Reports" icon, find "Print Last Session", tap it and press the Set button.

A copy of the report is also written to the CF drive. It is named <Log file name>.LOG.

Final Capture Report (Hardcopy Printout)

The hardcopy printout available on the Dossier was designed to provide sufficient information for use as an evidence identification tag. It contains information on the unit used to acquire the evidence, the personnel acquiring the evidence, and the important information for the actual capture session.

Information Format

This section describes the information format that appears on the Forensic Dossier hardcopy printouts.

For an example, see the included page at the end of this section.

Unit Information – The unit Information section identifies the model name of the acquiring unit, the unit serial number, and the software version installed.

Forensic Information – The Forensic Information section contains several lines for the user to enter the necessary information relevant to each investigation.

There are spaces for the following information:

- Evidence number and/or any alias identifier.
- The name of the person(s) acquiring the evidence.
- The date and time that the evidence was acquired.
- The location at the scene of the investigation where the evidence was acquired.
- A description of the acquired evidence.

Session Information – This section of the printout contains information specific to the actual Capture session.

Session Settings Information – This section contains information pertaining to the actual Session that is not specific to either drive. It contains the following:

- Operating Mode. This can be Capture, DD Capture, E01, Scan or Wipe clean.
- Verify. This reflects the Verify option setting for each operating mode as explained in previous sections of this text. When a DD capture is performed with Verify the Destination Hash Value is reported in the verify section of the audit trail report.
- Speed. This reflects the Speed option setting for each operating mode as explained previously.
- Connection. This is the connection method for the operating mode. This is meant to indicate whether a direct IDE, SATA or USB connection was used for the operating mode.
- Results. This line appears on the hardcopy only if the operating mode was Capture. It will contain one of the following lines.
 - “MIRROR COPY OF THE DRIVE HAS BEEN SUCCESSFULLY EXECUTED!”

- “SESSION RESULTS ARE INVALID BECAUSE THE OPERATION WAS ABORTED!”
- “SESSION RESULTS ARE INVALID BECAUSE THE OPERATION WAS IN ERROR!”
- Extra information. This line appears on the hardcopy only if the operating mode was Capture. It will contain one of the following lines:
 - The destination drive was verified as erased before Capture!
 - The destination drive was erased during the Capture!
 - Operator declined FULL destination drive erase and erased remainder.
 - Operator declined FULL and remainder destination drive erase!

Source drive Information – This section of the printout contains information specific to the Source or Suspect drive. This will only appear if the operating mode was (Native) Capture or DD Image Capture with Verify set to **HASH** or **HASH-Disk**. It contains the following:

- Drive Identification. These lines print the model and serial number as reported by the source drive.
- Physical Geometry. These lines indicate the number of cylinders, heads and sectors, the total number of sectors, and the drive size.
- HASH Value. This line prints the computed SHA-256 and MD5 values for the source drive.
- Error recovery information. These lines will only appear if the On Error setting for the Capture operation was set to something other than abort.

If the setting was set to “skip”, then a single line containing the total number of skipped sectors will be printed.

If the setting was “retry” or “recover”, two lines will be printed: One containing the total number of recovered sectors; one containing the total number of non-recovered or skipped sectors.

Destination drive Information – This section of the printout contains information specific to the destination drive. It contains the following.

- **Drive Identification.** These lines print the model and serial number as reported by the destination drive.
- **Physical Geometry.** These lines indicate the number of cylinders, heads and sectors, the total number of sectors, and the drive size.
- **HASH Value.** This line prints the computed SHA-256 and MD5 value for the destination drive. This will only appear if the operating mode was (Native) Capture with Verify set to **HASH**.
- **Media Verify information.** These lines will only appear if the operating mode was set to Scan. If after a Scan operation, any bad sectors, weak sectors, or weak spots are detected, then the addresses of those sectors are printed followed by the grand totals for each type.
- If one of the DD imaging modes was used with verify set to **HASH-File**, a list of file names with their respective SHA-256 and MD5 values will be printed at the bottom of the page.

Audit Trail Authentication Checksum – This number is used to verify if the report which resides on the CF Drive has not been altered in any way. The Checksum is a proprietary Hash value.

Note: The Audit Trail Authentication Checksum value is not a standard MD5 Hash value and it will not match the value calculated by third-party software or other means.

Keyword List – If a keyword search was performed during the capture, a list of the found keywords will appear at the very end of the Final Capture report.

Example of Hardcopy Printout

```

**** Forensic Dossier -- Serial No.:79198 -- ****
* Software: V2.2.1RC22 Firmware: V0.4.7 fs:NTFS *
* Time Zone: -8 Daylight Saving: +1 *
* Date: 05/02/2012 Time: 09:36:16 *
*
* Acquired by _____ Location _____ *
*
* Acquired on _____ AT _____ *
***** SESSION SETTINGS *****
* Operating Mode: 4G E01:S1=>D1 Address Mode: LBA *
* Verify : Hash-Disk Speed : UDMA-5 *
* Connection : Direct *
*
*
* E01 CAPTURE OF S1 HAS BEEN ACHIEVED.
*
***** SOURCE DRIVE(S) ***** DESTINATION DRIVE(S) *****
* S1 D1 *
* Model : WDC WD400JD-22LSA1 Model : ST380215AS *
* Serial: WD-WMAMAD178223 Serial: 9QZCBBKJ *
*
* C: 77545 H: 16 S: 63 C: 155061 H: 16 S: 63 *
* Total Sectors Drive Size Total Sectors Drive Size *
* 78165360 37.0GB 156301488 74.0GB *
*
*****
*** AD01.E01: S1: 0 To:10289151
* start MD5: 67452301 EFCDA889 98BADCFE 10325476
* end MD5: 5AE3BD87 7FE64ABA A0A579C1 242A46F2
*
*** AD01.E02: S1: 10289152 To:18587647
* start MD5: 5AE3BD87 7FE64ABA A0A579C1 242A46F2
* end MD5: A994FAC1 1FC5D1A1 8719127D BDE468BA
*
*** AD01.E03: S1: 18587648 To:26804223
* start MD5: A994FAC1 1FC5D1A1 8719127D BDE468BA
* end MD5: 942E9301 F89136F6 AE280697 5AA47A39
*
*** AD01.E04: S1: 26804224 To:35012607
* start MD5: 942E9301 F89136F6 AE280697 5AA47A39
* end MD5: 87B3AECF 162622E9 09DDAFD5 3BBC07FC
*
*** AD01.E05: S1: 35012608 To:43278335
* start MD5: 87B3AECF 162622E9 09DDAFD5 3BBC07FC
* end MD5: 68F3686E 0547026F 731F677F F40835C4
*
*** AD01.E06: S1: 43278336 To:51470335
* start MD5: 68F3686E 0547026F 731F677F F40835C4
* end MD5: 9DE9BE75 8658CF30 8F43ABDF EFFBA058
*
*** AD01.E07: S1: 51470336 To:59670527
* start MD5: 9DE9BE75 8658CF30 8F43ABDF EFFBA058
* end MD5: 70141F64 6738FA0D 085FA55A D4286DFB
*
*** AD01.E08: S1: 59670528 To:68042751
* start MD5: 70141F64 6738FA0D 085FA55A D4286DFB
* end MD5: C0727107 59261AB6 8DCE2FB1 CE3971B7
*
*** AD01.E09: S1: 68042752 To:78165359
* start MD5: C0727107 59261AB6 8DCE2FB1 CE3971B7
* end MD5: A5E70491 584454D4 1E297503 96B6426E
*
*** S1 From: 0, To: 78165359, Size: 78165360
* Source MD5:
* ...E3484EA1 7B173D50 4AFE530D 8AFE89F4...
*
*****
*
* Skipped Sectors: 0 Recovered Sectors: 0
*
*****
Compression Ratio is : 1.07 : 1
Completion Time: 05/02/2012 09:52:29
Audit Trail Checksum: 53A8C874 062934A9 2B538A42 D491922B

```

12. Frequently Asked Dossier Questions and Answers

- Q.** Does the Dossier support drives larger than 2TB in capacity?
- A.** Yes, the Dossier supports drives larger than 2TB in capacity.
- Q.** By comparison my Dossier appears to be operating slower than other units.
- A.** Make sure that your unit is using the latest software. Visit <http://www.logicube.com> and go to the support page to view the latest software level and if necessary download the software for your system.
- Q.** My Dossier continues to ask if I want to wipe a brand new capture HDD.
- A.** This is a normal Dossier question that will be asked unless the new HDD is wiped by the Dossier. Using the Dossier to prepare (pre-wipe) a new Destination HDD will eliminate this screen from displaying while on site thus speeding up the capture process.
- Q.** After installing a brand new destination drive in my Dossier and starting a capture, I received a message that the drive was not erased, is this normal?
- A.** Even though new drives are usually blank, they still need to be wiped to guarantee that they do not contain any data. The Dossier writes a signature to the destination drive during the wipe session. It is this signature that tells the Dossier that the destination or capture drive was previously wiped. Destination drives can be prepared ahead of time by wiping them with signature set to "YES".
- Q.** Can I make bootable "Clone" with the Dossier?
- A.** While the Dossier was not designed to produce a bootable "clone", it will create a copy of the source drive with bit-for-bit accuracy. Whether or not the destination drive will boot depends upon many factors that include drive geometry, operating systems, and PC BIOS issues.
- Q.** On my capture drive the information displayed on the Dossier does not agree with the label fixed to the target HDD. Example: The number of cylinders displayed is different than the label
- A.** This issue has come up on Seagate HDDs. Although the information displayed may not agree, the correct information will be on the printed report generated at the end of the capture session.
- Q.** Drive information as displayed on the Dossier does not agree with the label fixed to the target HDD. Example: The number of cylinders displayed is different than the label
- A.** Drive labels will only show Cylinders, Heads, and Sectors for a maximum of 8.5GB (example: 16383, 16, 63.) The actual drive parameters will be displayed both in drive information, and in the printed session report. Most of the newer drives only have an LBA (Logical Block Addressing) value printed on the label showing the drive's capacity in sectors

- Q.** Capturing data from a Western Digital HDD is not working.
- A.** Most Western Digital drives require that the jumpers be removed for a capture to work. The exception to this statement is for the Western Digital "Xpert" series Hard Drives (an older manufactured version), where the jumper is set to the master position.
- Q.** I'm trying to update my Dossier with the latest software but I cannot get my PC to communicate with the unit.
- A.** Make sure that the PC is either connected through the USB or FireWire port.
- Q.** Will DD Image capture files have the same "odd sector" problem of the Linux operating system?
- A.** Although DD Image capture files are formatted as "DD Linux" files, they do not utilize the Linux kernel. The Linux OS is unable to see the last sector of a drive that has an odd number of sectors. Some users have asked if this problem will prevent the last sector of an odd sector drive from being captured. The answer is no.
- Q.** What happens if a HASH mismatch occurs during a Mirror or DD capture with verification on?
- A.** The capture session will immediately abort and this message will be displayed on the Dossier:
- Error**
Error Capturing Drive! Drive error.
Either the speed setting is too high
Or a bad sector was found!
- Q.** What will happen if a drive cable makes intermittent contact during a capture?
- A.** The capture session will immediately abort and an error message will be displayed on the Dossier display.
- Q.** If a verification mismatch occurs during a capture will the clone complete?
- A.** No. The capture session will immediately abort and display an error message on the Dossier indicating that an error has occurred. A Log file is not generated when a mismatch occurs.
- Q.** When two drives are created from one source drive as a DD image with Disk + Verification turned ON how do I know both copies have been verified by Dossier to be exactly the same as the source?
- A.** If at any time during the capture either of the two copies encounters a hash mismatch as part of the verification process, Dossier will terminate the capture before the log file can be created. If the capture completes successfully the SHA- 256 and MD5 digests for S1 will be displayed on Dossier and in the log file along with the message AN EXACT DD IMAGE FILE COPY OF S1 HAS BEEN ACHIEVED.
- Q.** Does the Dossier support E01 file format?

- A. Yes, the Dossier has an optional feature to capture suspect drive data in the E01 file format. It can be used with Encase ver.6.X and with Access Data's FTK Imager v3.X

13. Index

1.5 gigabits per second, 85
 Administrative functions, 84
 Alphanumeric Keypad, 25, 30, 46, 47, 48
 ATA T13 Security, 53
 BIOS, 43, 63, 117
 Bootable CD-ROM, 13, 87
Browse Destination Setting, 51, 52
Button, BACK, 25, 50, 79
 Button, Reset, 23
 Button, SELECT, 26, 30, 46, 47, 48, 52, 112
 Button, SET, 23, 25, 29, 30, 45, 46, 47, 48, 66, 67, 74, 75, 99, 112
Button, START/STOP, 24, 45, 88
 Capture, DD Image – 650MB, 27
 Capture, Native, 27, 28, 46
 CARDBUS, 86
 Case File, 32, 36
 Chkdsk, Microsoft Windows, 51
 cholesteric display, 80
 CIFS, 84
 Clone, 27, 30, 39, 63, 68, 80, 86, 87, 112, 117
 Clone Card Pro™, 11, 80, 86, 87, 89, 92, 95
 credentials, 84
 Cylinders, 114, 115, 117
 Date & Time, 23
 Daylight Saving, 62
DD Image, 27
 DD Linux Image File, 118
 Disclaimer, Liability Limitation, II
 Disk Control Overlay (DCO), 43, 44
 Disk, Floppy, 87
 Display, LCD, 22
 Dossier® tray, 84, 85
Drive Defect Scan, 28, 44, 45, 105
 Drive, CD-ROM, 12, 13, 33, 65, 86, 87, 88, 102
 Drive, Destination, 9, 10, 12, 13, 17, 27, 28, 30, 32, 36, 39, 42, 105, 106, 107, 108, 109, 110, 111, 112, 114, 115, 117
 Drive, IDE, 17, 18, 113
 Drive, Jumper Setting, 19, 20, 118
 Drive, older, 41
Drive, Quantum, 20
 Drive, Serial ATA (SATA), 12, 13, 17, 18, 20, 21
 Drive, Source, 27, 28, 105, 107, 108, 109, 110, 112, 114, 117
 Drive, Suspect, 9, 10, 12, 13, 18, 19, 27, 28, 30, 42, 74, 86, 114
Drive, Western Digital, 20, 118
 Drives, External USB, 22, 33
 Drives, SCSI, 22
E01, 27, 34
 E01 Resume, 24, 61
 Encase™, Guidance Software, 27, 33
Erase™ Target Mode, 46
Error, Source Data Lines not Verified, 110
 eSATA, 81
 EU, EUROPEAN UNION, III
 Evidence, 9, 16, 18, 20, 39, 46, 112, 113
 file access protocols, 84
 Final Capture Report, 30, 42, 43, 75, 76, 110, 112, 115

- Firewire (1394), 11, 12, 13, 28, 30, 33, 45, 65, 67, 99, 100, 118
- Forensic Dossier, 84, 85
- Forensic Dossier®, 84, 85
- Forensic MD5™ Kit, 9
- FREEDOS, 87
- FTK™, 27, 67, 68
- Geometry, Drives, 26, 114, 115, 117
- Hard Drive, Western Digital, 118
- hardware, 82
- HDD, Hard Disk Drive, 9, 12, 13, 117, 118
- Host Protected Area (HPA), 43, 44
- iLook™, 27, 67, 68
- Indicator Lights, 25
- install hard disk, 82
- Install Options, 60
- JBOD, 81
- Keyword Search, 11, 28, 43, 44, 45, 52, 64, 74, 75, 76, 77, 78, 99
- Keywords, Case, 77
- Keywords, Signature, 76, 77
- Keywords, Unicode, 10, 77
- Languages, 61
- Light, Error**, 25, 114
- Light, Power**, 25
- Light, Status**, 25, 47
- Linux, 77, 118
- Mac, 77
- Macro, 84
- Manage Destination Menu, 26, 50, 51, 53
- Massive Portable Forensic Storage. See MPFS
- MD5 Hash, 10, 30, 32, 36, 43, 48, 106, 115
- Mode, Security Erase**, 46, 47, 106
- Modify Lists, Keyword Setting**, 77, 78
- mounting brackets, 82
- MPFS, 80, 81, 82, 83, 84
- MPFS™, 84
- NETConnect, 80, 81, 84, 85, 86
- Network, 84
- Network protocols, 84
- NFS, 84
- On Error, Abort, 42, 107
- On Error, Recover, 42, 107
- On Error, Retry, 42, 107
- On Error, Skip, 42, 107
- Optional Preference Settings, 29, 31, 35, 39
- Paper, Thermal, 38
- Partition, FAT32, 51, 52
- PCMCIA, 13, 86, 87
- PCMCIA slot, 87
- Portable Battery Pack, 89, 92, 95
- Power Supply, 93, 94, 96, 97
- Printer, 30, 32, 36, 38, 46, 48, 49, 52, 108, 112
- Printer, Brother MW-120™, 38
- Printer, Pentax Pocketjet 200™, 38
- QWERTY, 11
- RAID, 11, 63
- real time clock, 23
- Recalibrate Touch Screen, 22
- Report, Print Search Detail**, 52, 75, 76
- Report, Print Search Text**, 52, 75, 76
- RoHS Directive (2002/95/EC), III
- SAS Adapter**, 95
- Scandisk Setting, 51
- Scandisk, Microsoft Windows**, 51
- Scratch drive, 12
- Screen, Main Menu, 26
- Screen, Settings, 27, 29, 38, 45, 46, 48, 49, 75, 77
- Screen, Touch, 22
- SCSI Adapter**, 92
- SCSI/SAS, 57
- Sector, bad, 28, 40, 42, 43, 45, 46, 48, 105, 106, 107, 115
- Sector, weak, 40, 45, 46, 106, 115
- Set button**, 25
- Setting, On Error, 29, 31, 35, 42, 43, 107, 114
- Setting, Speed, 40, 44, 88, 106
- Setting, Verify, 29, 31, 33, 35, 39, 40, 64, 106, 111, 113, 114, 115
- Software, Loading, 99, 102
- Spanning, 40
- Specifications, 9
- Speed benchmarking, 41
- Speed, PIO-Auto**, 41
- Speed, PIO-Medium, 41, 88
- Speed, PIO-Slow**, 41
- Speed, UDMA-0, 106
- Speed, UDMA-3**, 41
- Speed, UDMA-4**, 41
- Speed, UDMA-5**, 41
- Speed, UDMA-6, 106
- Technical Support, Logicube, III, 22, 27, 121
- Telnet, 84
- Time Zone, 61
- Touch Screen, 22, 23, 24, 25

Unix, 77
 USB 1.x, 65, 68
 USB Cloning Option, 68, 69
 USB Port, 12, 13, 28, 33, 65, 66, 68
 User interface (UI), 22
 Verification, CRC-32, 106
 Verification, Hardware CRC32, 106
 Verification, Hardware MD5, 106
Verification, MD5-Disk, 33, 114
Verification, MD5-File, 33, 115
 Verification, Software CRC32, 106
 Warranty, Parts and Labor, II, III
 Website, Logicube, III, 60, 99, 102, 117
 WipeClean™ Destination, 46
WipeClean™ Destination Mode, 45, 46, 47

Technical Support Information

For further assistance please contact
 Logicube Technical Support at: **(001) 818 700 8488 7am-5pm PST, M-F**
(excluding US legal holidays)
 or by email to **techsupport@logicube.com**